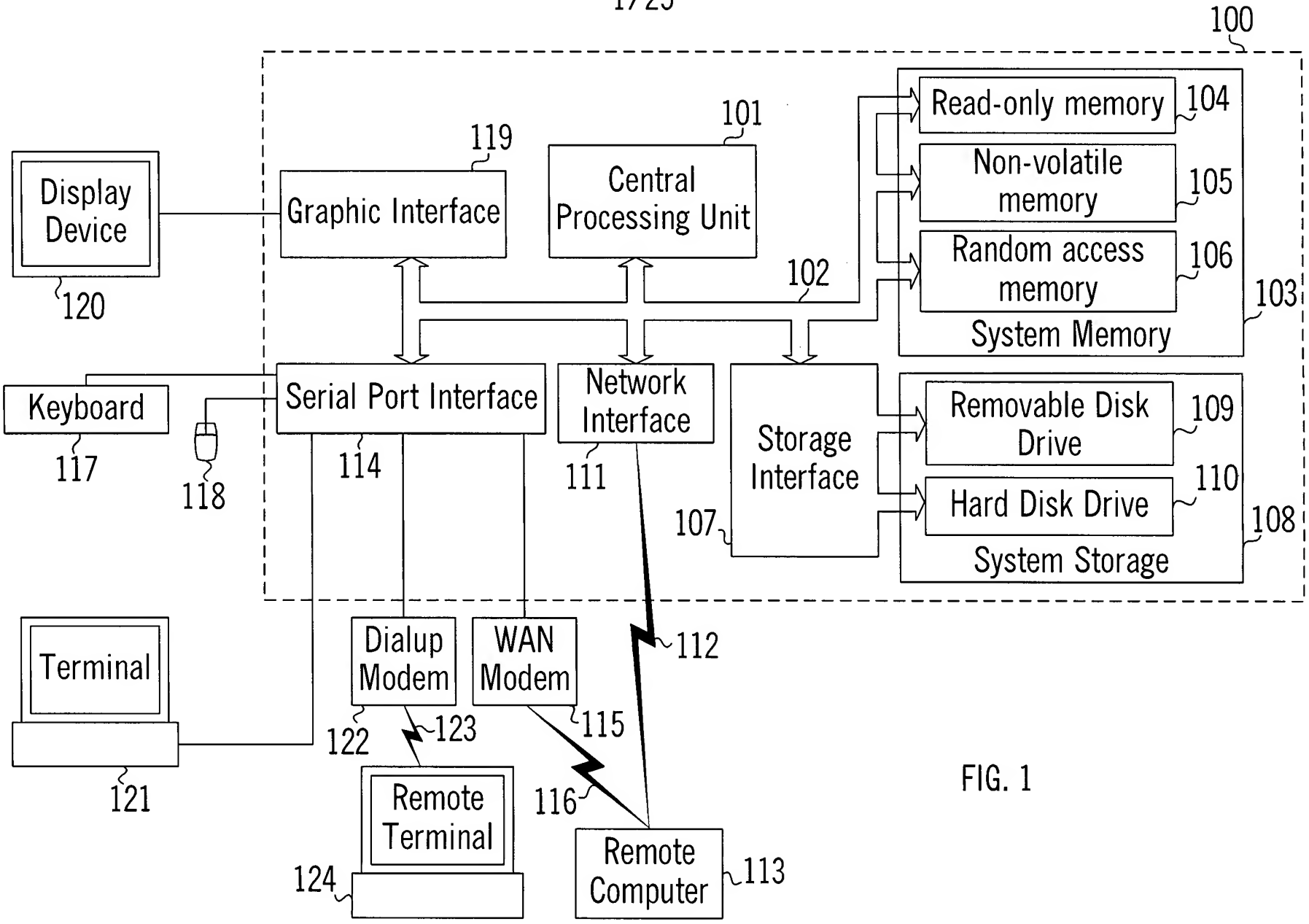
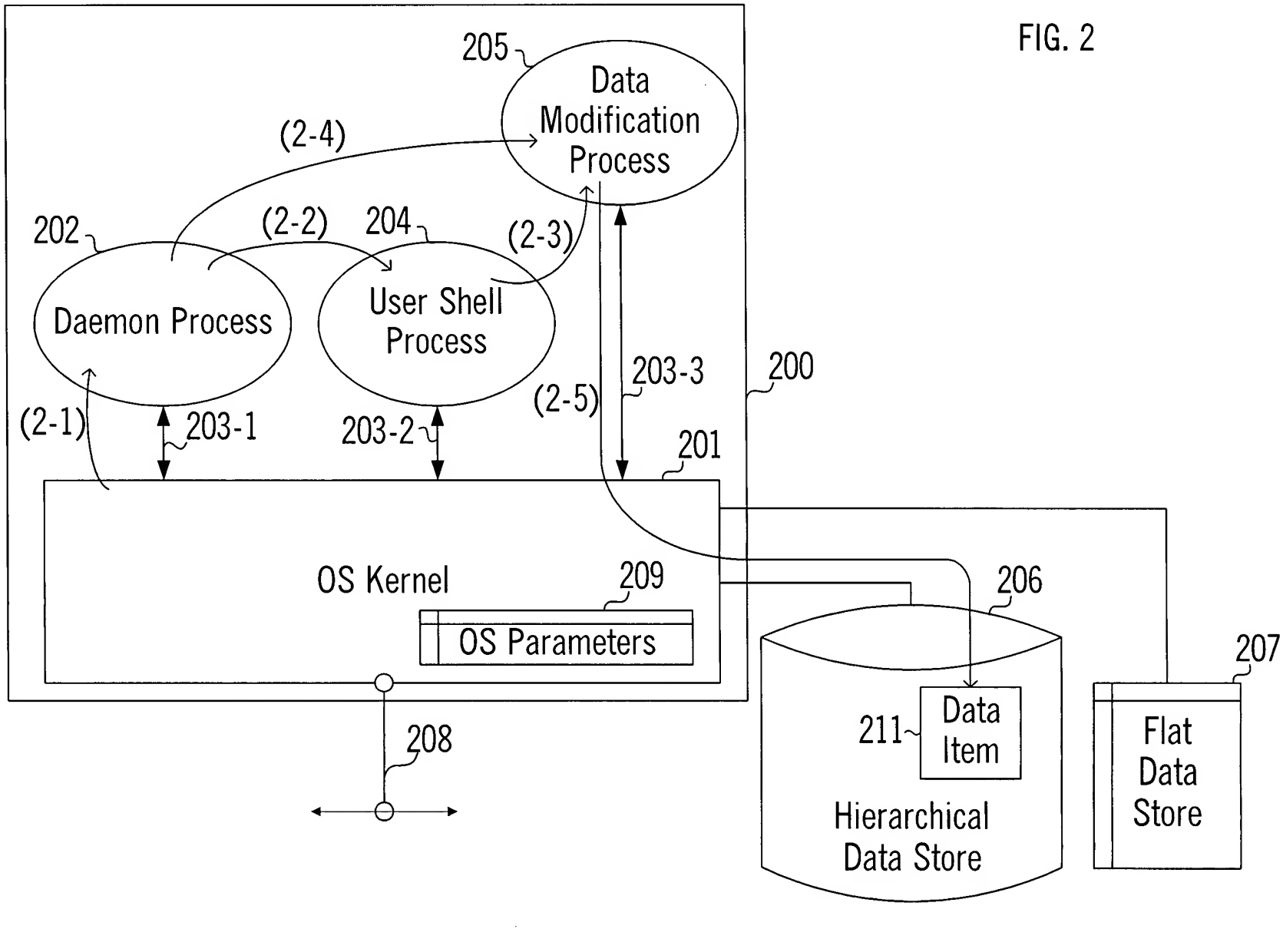

100
Read-only memory
104
Non-volatile memory
105
Random access memory
106
System Memory
103
101
Central Processing Unit
119
Graphic Interface
Display Device
120
102
Keyboard
117
118
Serial Port Interface
114
Network Interface
111
Storage Interface
107
Removable Disk Drive
109
Hard Disk Drive
110
System Storage
108
112
Terminal
121
Dialup Modem
122
123
WAN Modem
115
116
Remote Terminal
124
Remote Computer
113

FIG. 1

FIG. 2


205
Data Modification Process
(2-4)
202
(2-2)
204
(2-3)
Daemon Process
User Shell Process
200
203-3
(2-5)
(2-1)
203-1
203-2
201
OS Kernel
209
206
OS Parameters
207
211
Data Item
208
Hierarchical Data Store
Flat Data Store

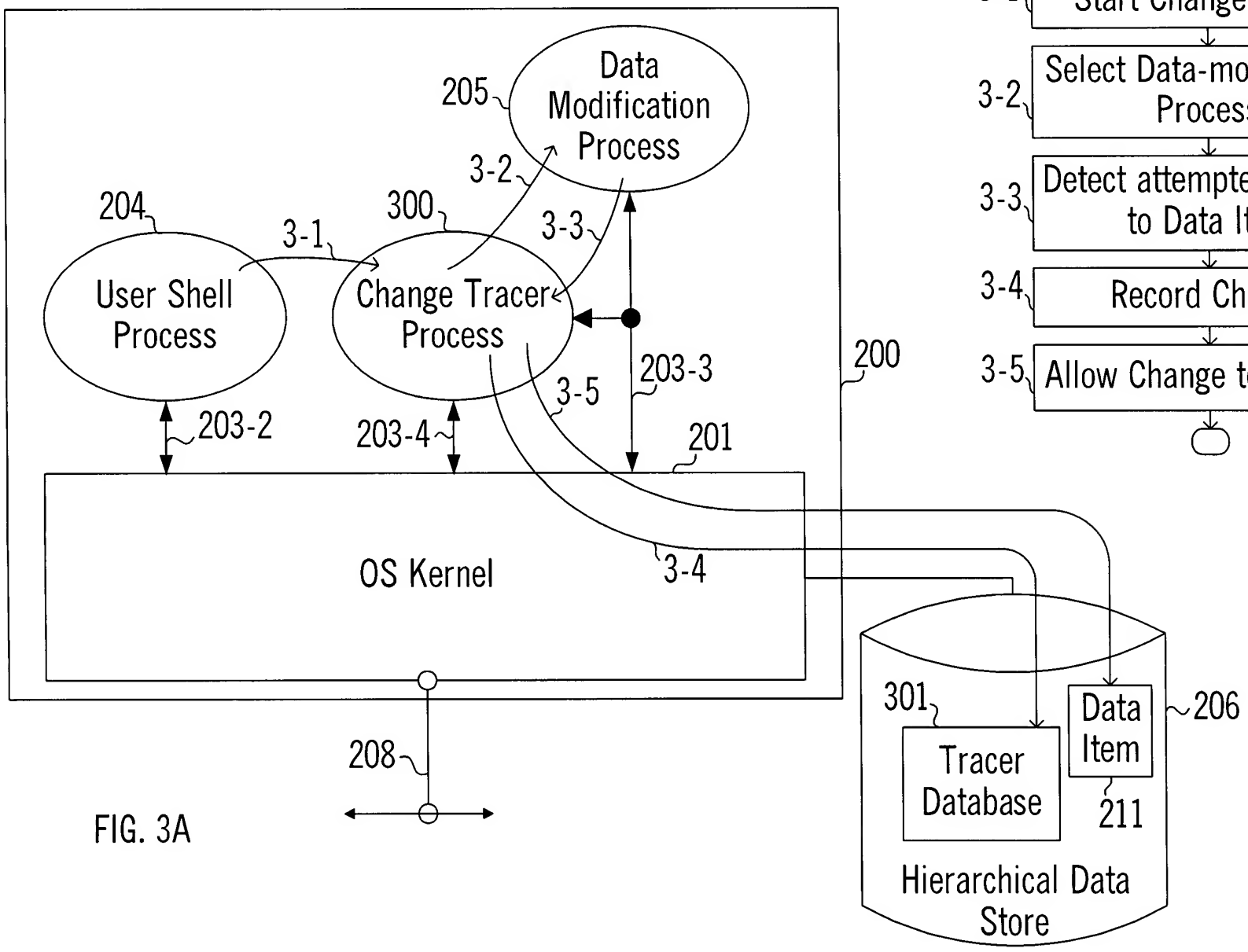

205
Data Modification Process
3-2
204
300
3-1
3-3
User Shell Process
Change Tracer Process
200
203-3
3-5
203-2
203-4
201
OS Kernel
3-4
301
Data Item
206
Tracer Database
211
Hierarchical Data Store
208

FIG. 3A

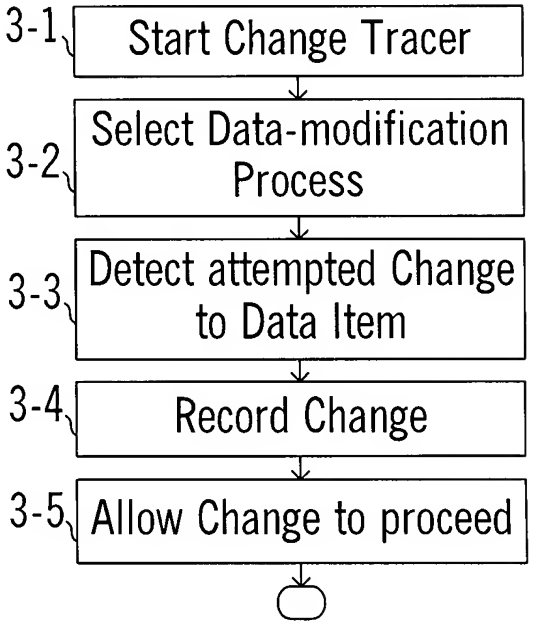

3-1
Start Change Tracer
3-2
Select Data-modification Process
3-3
Detect attempted Change to Data Item
3-4
Record Change
3-5
Allow Change to proceed

FIG. 3B

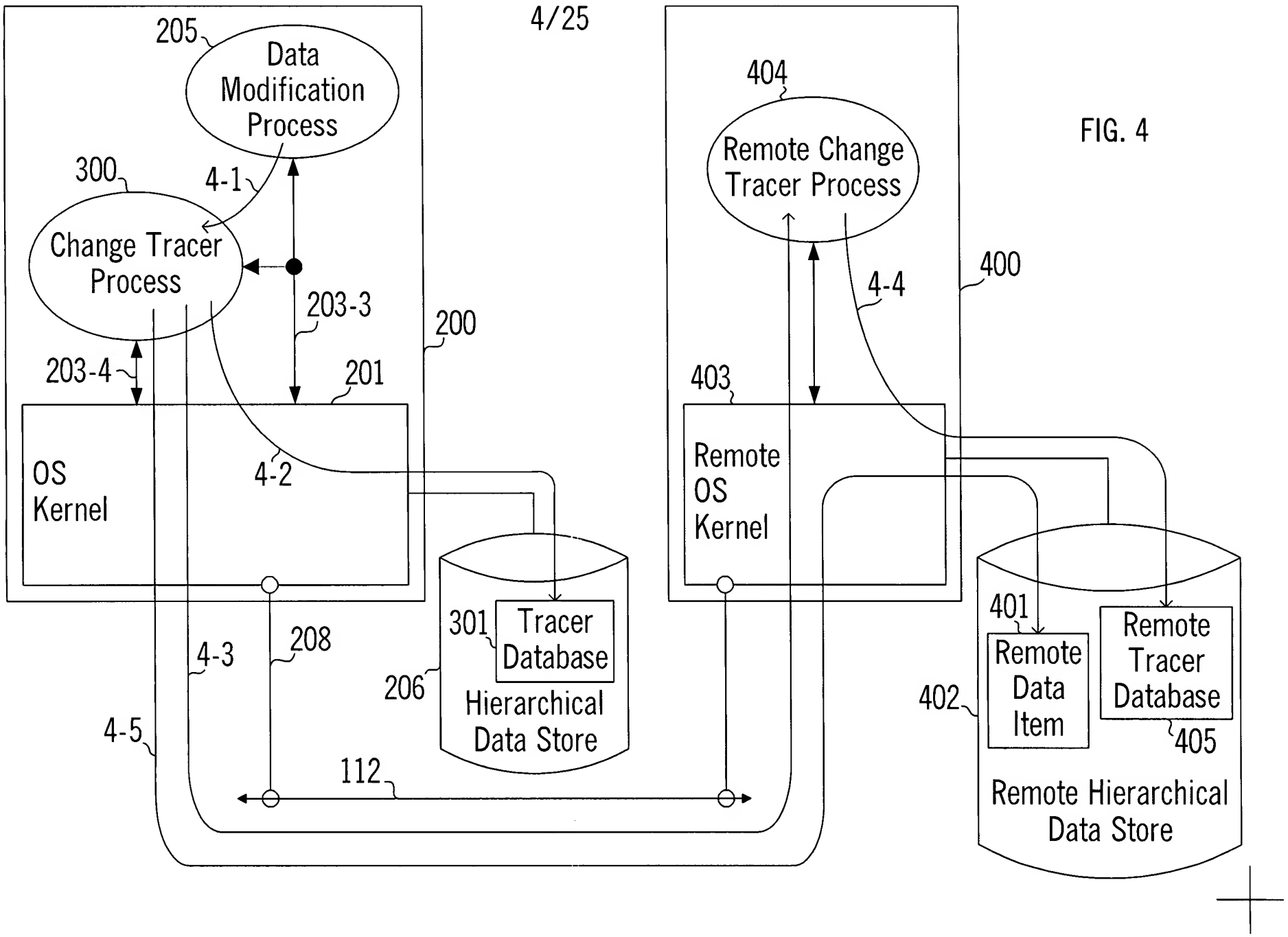

205
Data Modification Process
300
4-1
Change Tracer Process
203-3
200
203-4
201
OS Kernel
4-2
208
4-3
4-5
206
301
Tracer Database
Hierarchical Data Store
112
404
Remote Change Tracer Process
400
4-4
403
Remote OS Kernel
401
Remote Data Item
Remote Tracer Database
405
402
Remote Hierarchical Data Store

FIG. 4

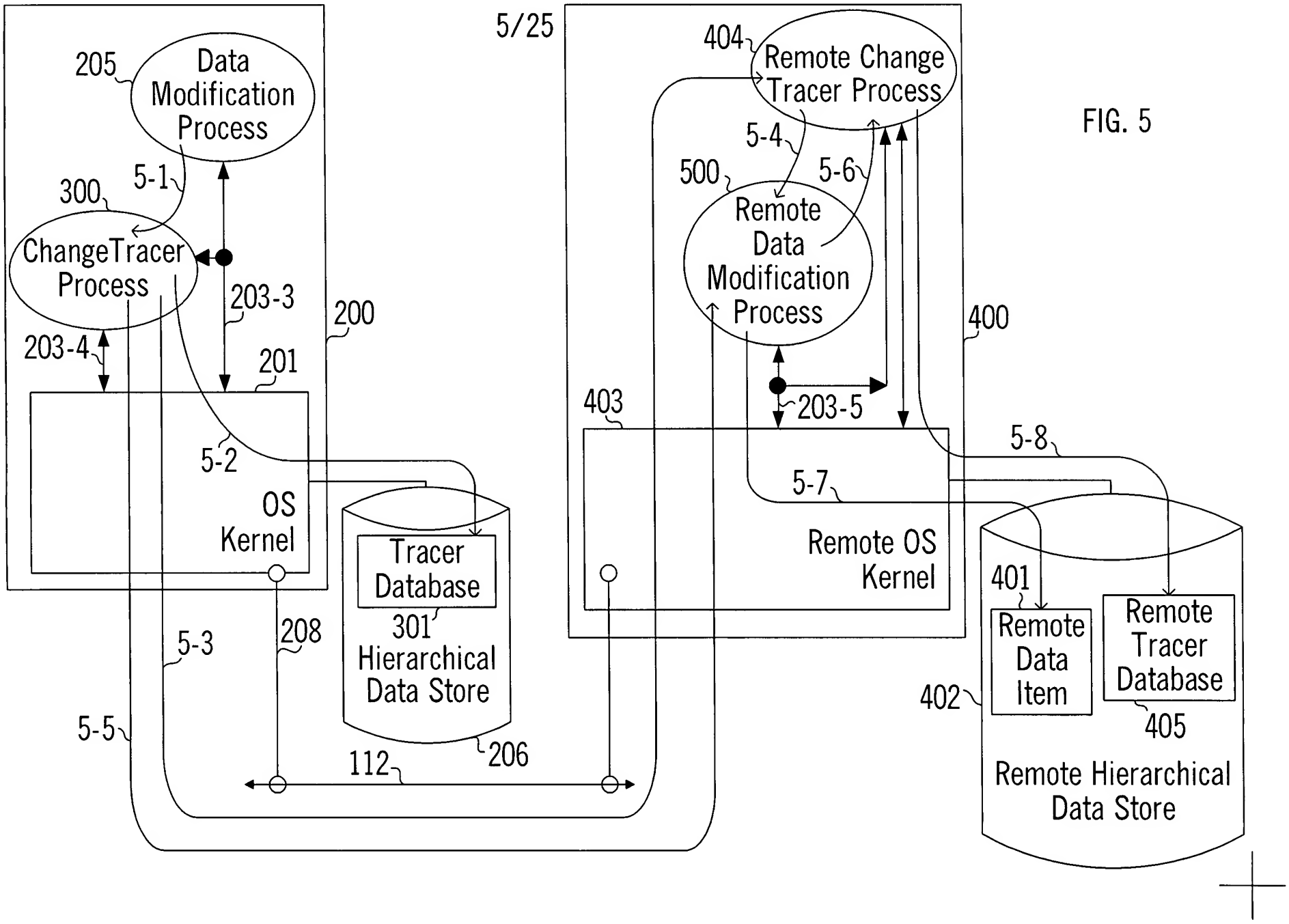

205
Data Modification Process
5-1
300
ChangeTracer Process
203-3
200
203-4
201
5-2
OS Kernel
Tracer Database
301
Hierarchical Data Store
206
208
5-3
5-5
112
404
Remote Change Tracer Process
5-4
5-6
500
Remote Data Modification Process
400
203-5
403
5-8
5-7
Remote OS Kernel
401
Remote Data Item
Remote Tracer Database
405
402
Remote Hierarchical Data Store

FIG. 5

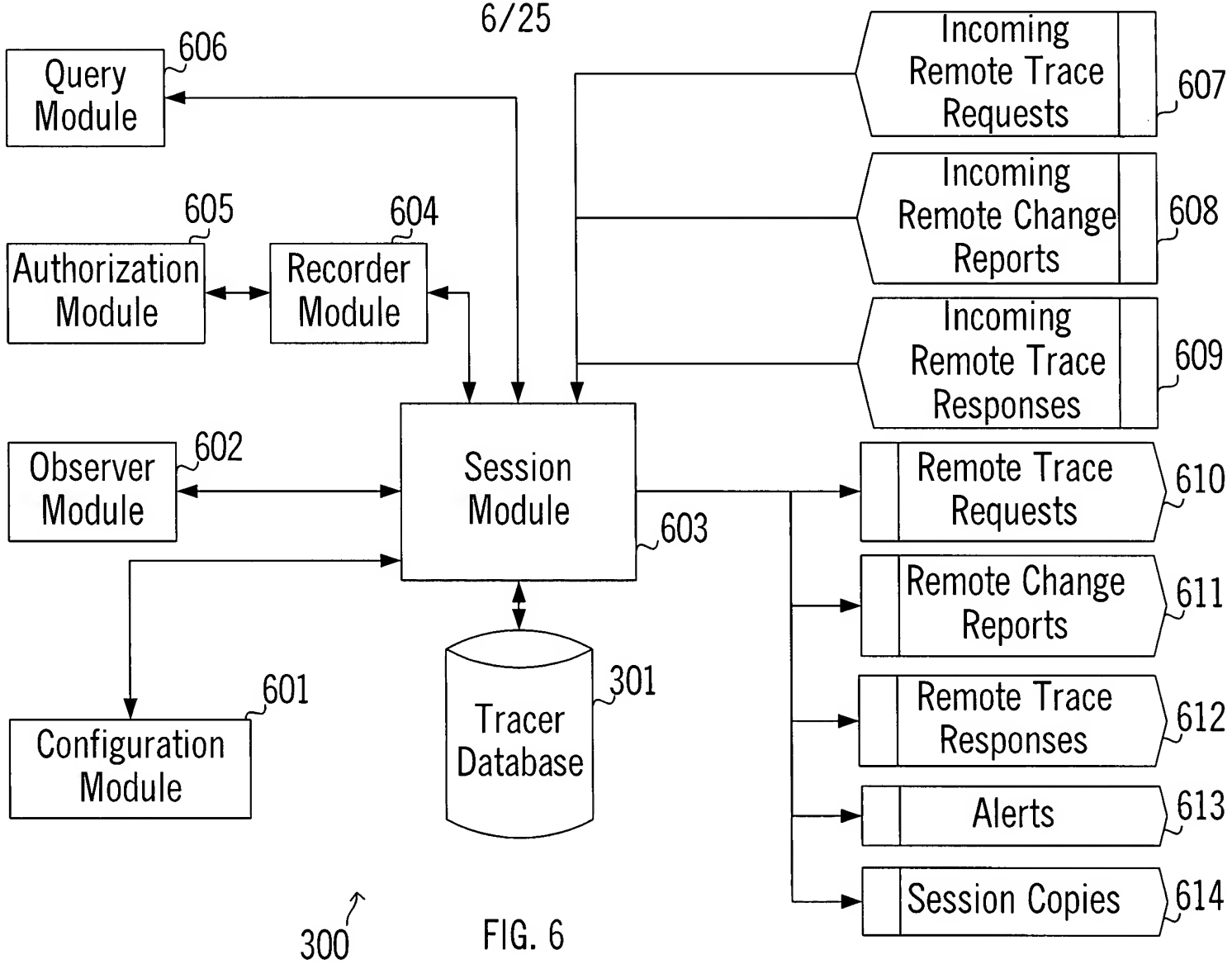

Query Module
606
Authorization Module
605
Recorder Module
604
Observer Module
602
Session Module
603
Configuration Module
601
Tracer Database
301
Incoming Remote Trace Requests
607
Incoming Remote Change Reports
608
Incoming Remote Trace Responses
609
Remote Trace Requests
610
Remote Change Reports
611
Remote Trace Responses
612
Alerts
613
Session Copies
614
300

FIG. 6

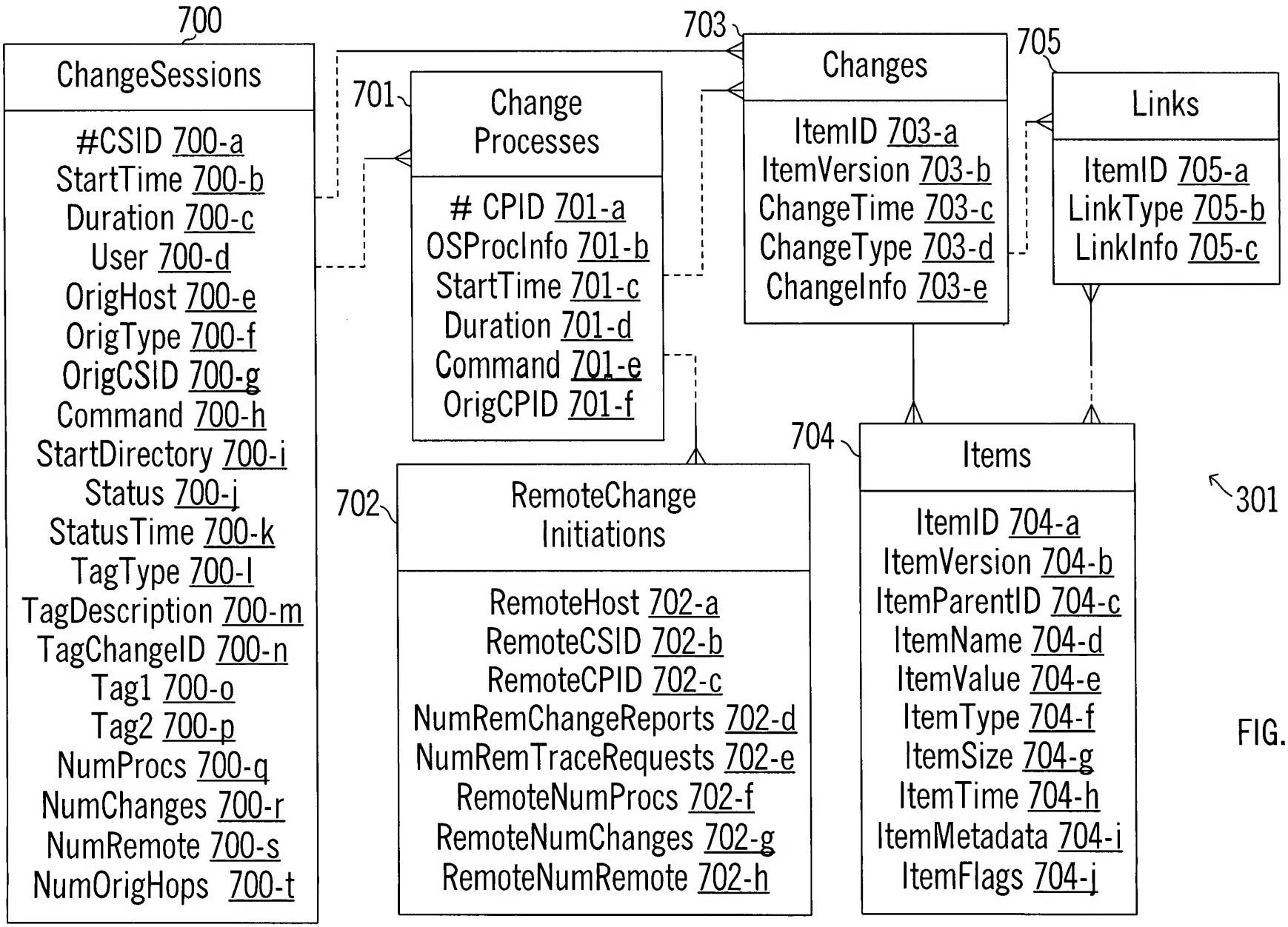

700
ChangeSessions
#CSID 700-a
StartTime 700-b
Duration 700-c
User 700-d
OrigHost 700-e
OrigType 700-f
OrigCSID 700-g
Command 700-h
StartDirectory 700-i
Status 700-j
StatusTime 700-k
TagType 700-l
TagDescription 700-m
TagChangeID 700-n
Tag1 700-o
Tag2 700-p
NumProcs 700-q
NumChanges 700-r
NumRemote 700-s
NumOrigHops 700-t
701
Change Processes
CPID 701-a
OSProcInfo 701-b
StartTime 701-c
Duration 701-d
Command 701-e
OrigCPID 701-f
702
RemoteChange Initiations
RemoteHost 702-a
RemoteCSID 702-b
RemoteCPID 702-c
NumRemChangeReports 702-d
NumRemTraceRequests 702-e
RemoteNumProcs 702-f
RemoteNumChanges 702-g
RemoteNumRemote 702-h
703
Changes
ItemID 703-a
ItemVersion 703-b
ChangeTime 703-c
ChangeType 703-d
ChangeInfo 703-e
704
Items
ItemID 704-a
ItemVersion 704-b
ItemParentID 704-c
ItemName 704-d
ItemValue 704-e
ItemType 704-f
ItemSize 704-g
ItemTime 704-h
ItemMetadata 704-i
ItemFlags 704-j
705
Links
ItemID 705-a
LinkType 705-b
LinkInfo 705-c
301

FIG. 7

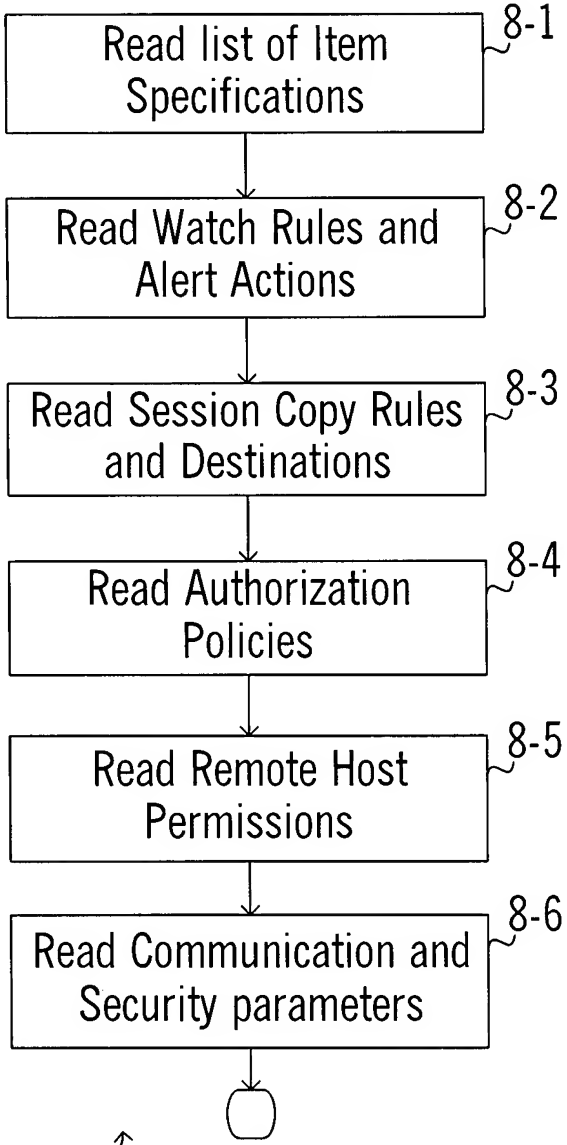

Read list of Item Specifications
8-1
Read Watch Rules and Alert Actions
8-2
Read Session Copy Rules and Destinations
8-3
Read Authorization Policies
8-4
Read Remote Host Permissions
8-5
Read Communication and Security parameters
8-6
601

FIG. 8

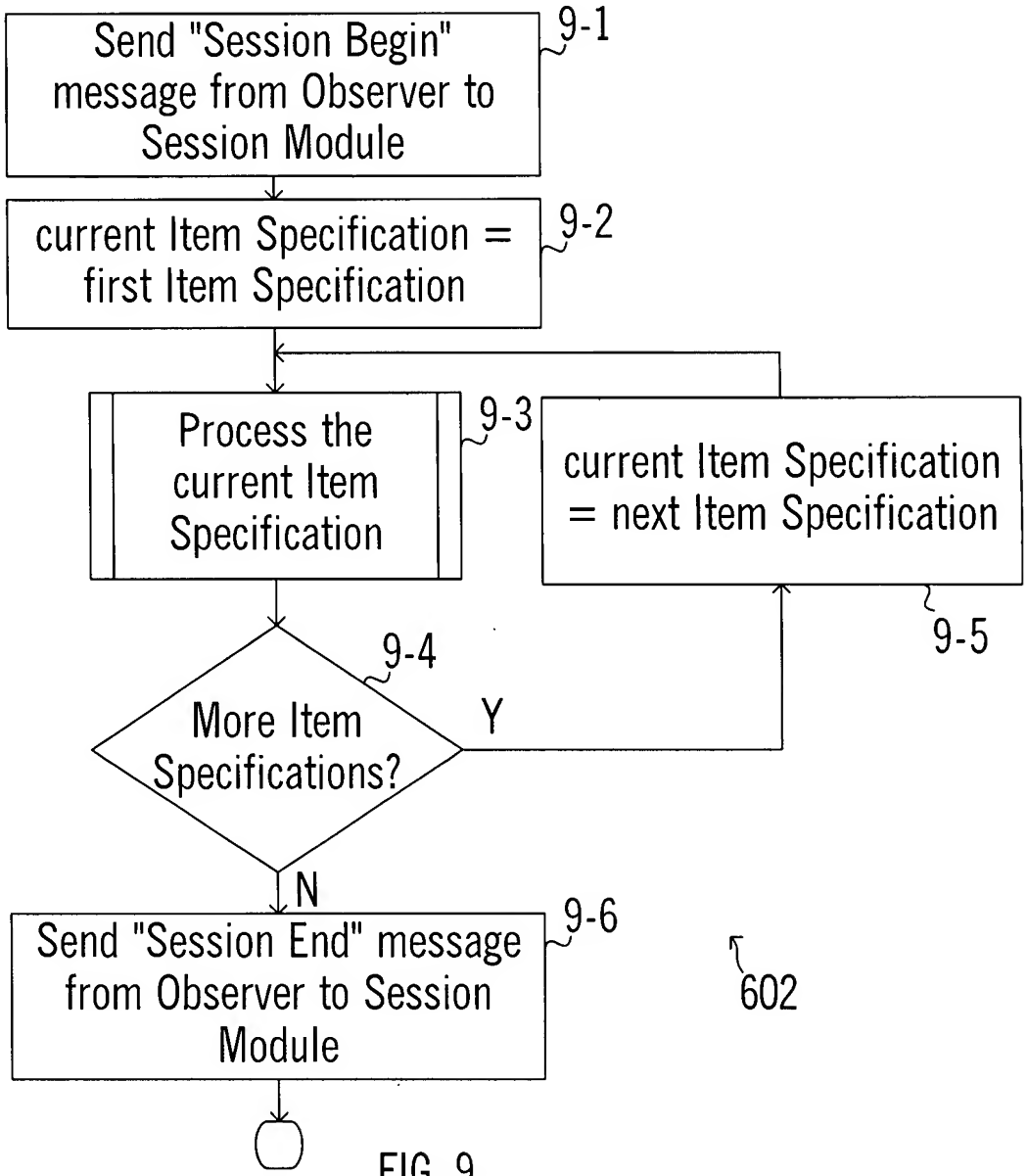

Send "Session Begin" message from Observer to Session Module
9-1
current Item Specification = first Item Specification
9-2
Process the current Item Specification
9-3
current Item Specification = next Item Specification
9-5
More Item Specifications?
9-4
Y
N
Send "Session End" message from Observer to Session Module
9-6
602

FIG. 9

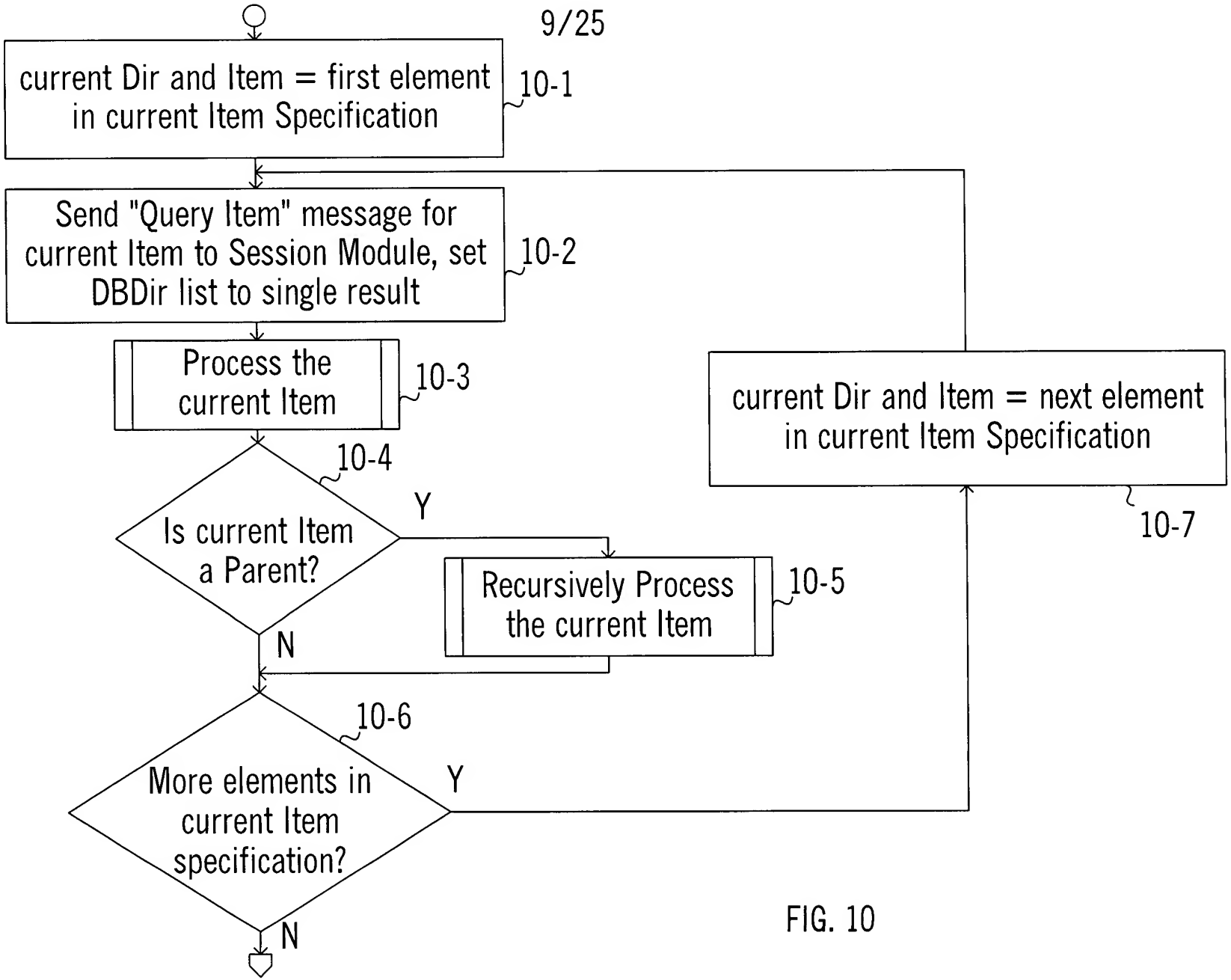
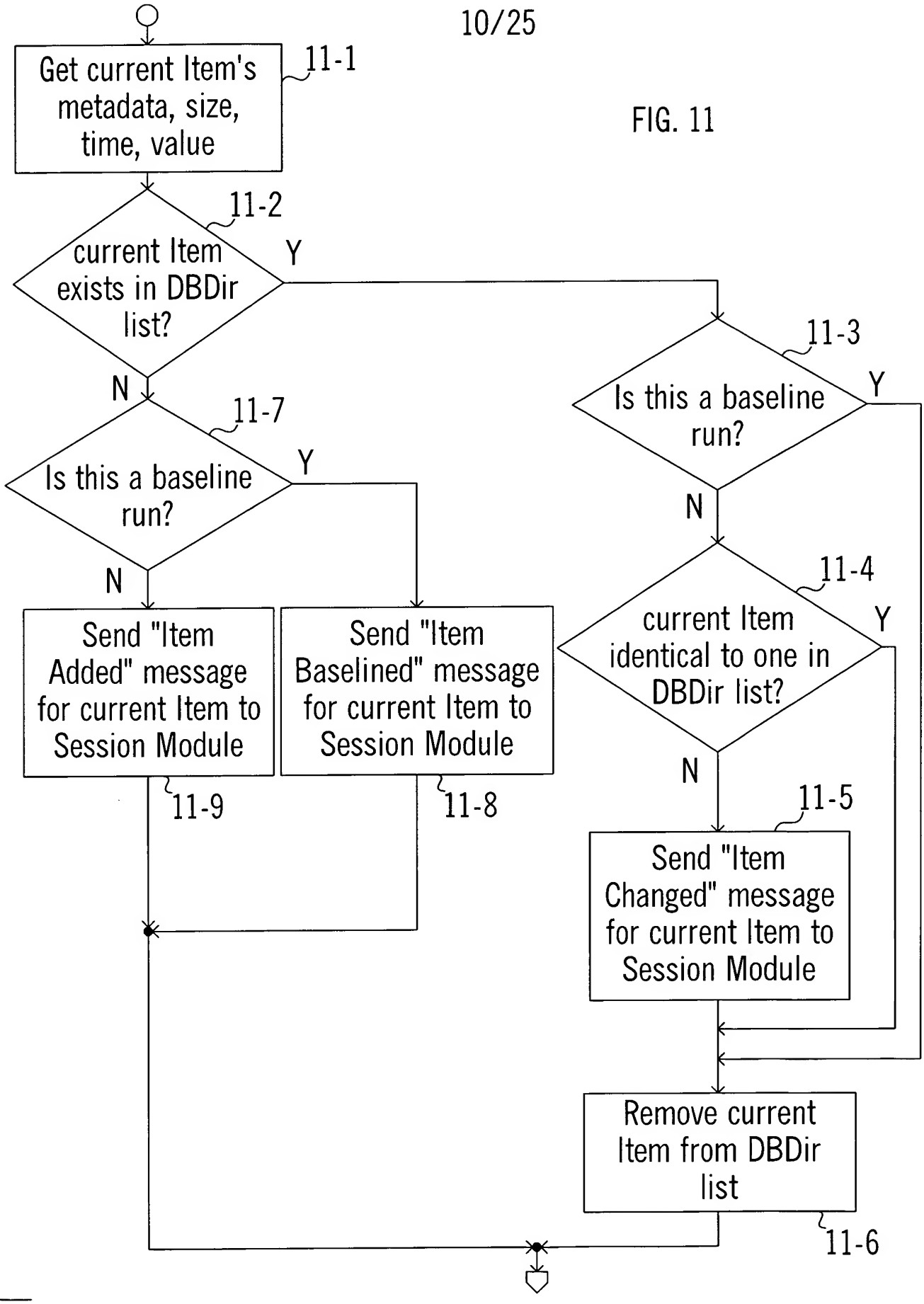

current Dir and Item = first element in current Item Specification
10-1
Send "Query Item" message for current Item to Session Module, set DBDir list to single result
10-2
Process the current Item
10-3
10-4
Is current Item a Parent?
Y
Recursively Process the current Item
10-5
N
10-6
More elements in current Item specification?
Y
N
current Dir and Item = next element in current Item Specification
10-7

FIG. 10

FIG. 11


Get current Item's metadata, size, time, value
11-1
current Item exists in DBDir list?
11-2
Y
N
Is this a baseline run?
11-3
Y
N
current Item identical to one in DBDir list?
11-4
Y
N
Send "Item Changed" message for current Item to Session Module
11-5
Remove current Item from DBDir list
11-6
Is this a baseline run?
11-7
Y
N
Send "Item Added" message for current Item to Session Module
11-9
Send "Item Baselined" message for current Item to Session Module
11-8

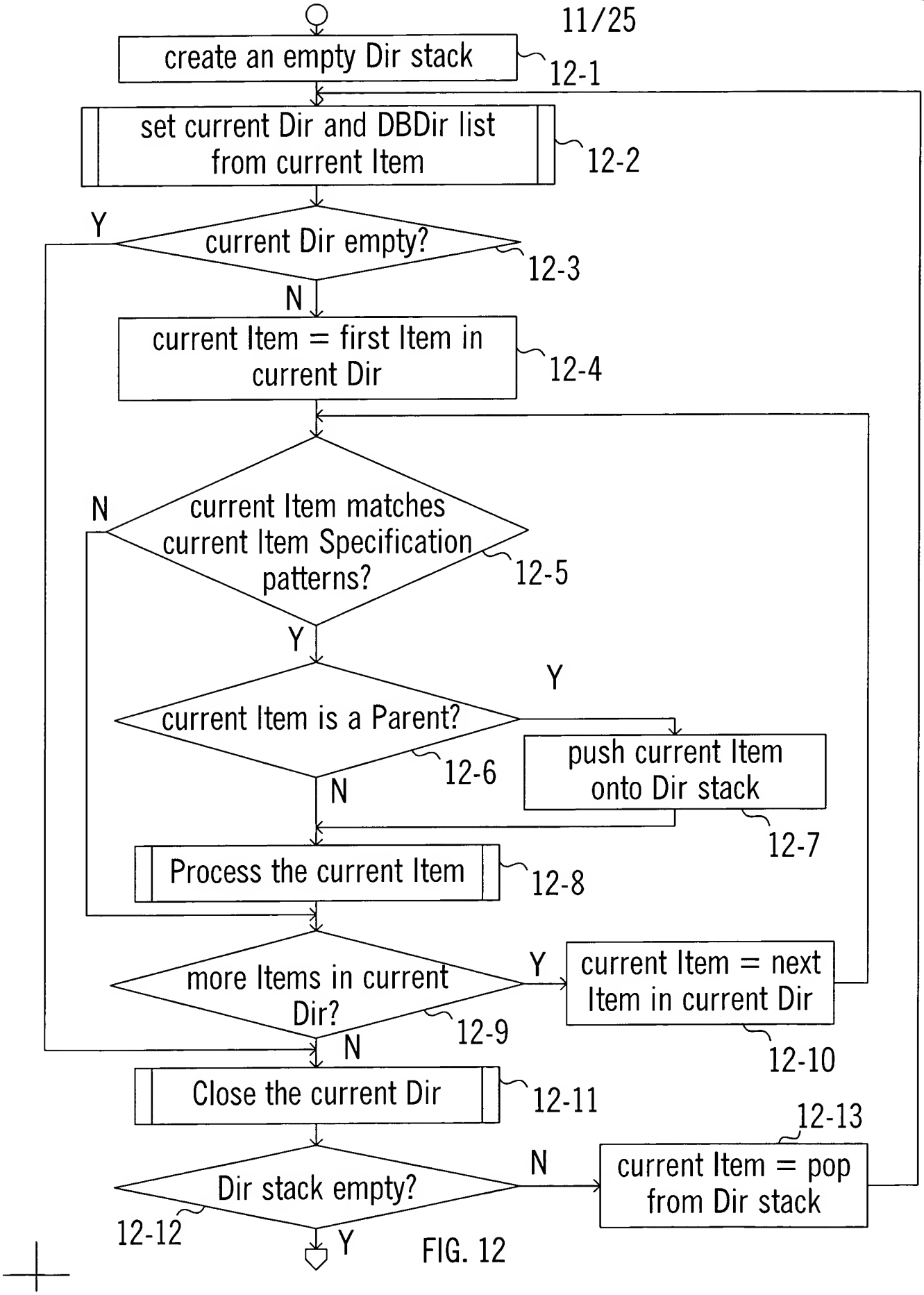

create an empty Dir stack
12-1
set current Dir and DBDir list from current Item
12-2
current Dir empty?
Y
N
12-3
current Item = first Item in current Dir
12-4
current Item matches current Item Specification patterns?
N
Y
12-5
current Item is a Parent?
Y
N
12-6
push current Item onto Dir stack
12-7
Process the current Item
12-8
more Items in current Dir?
Y
N
12-9
current Item = next Item in current Dir
12-10
Close the current Dir
12-11
Dir stack empty?
N
Y
12-12
current Item = pop from Dir stack
12-13

FIG. 12

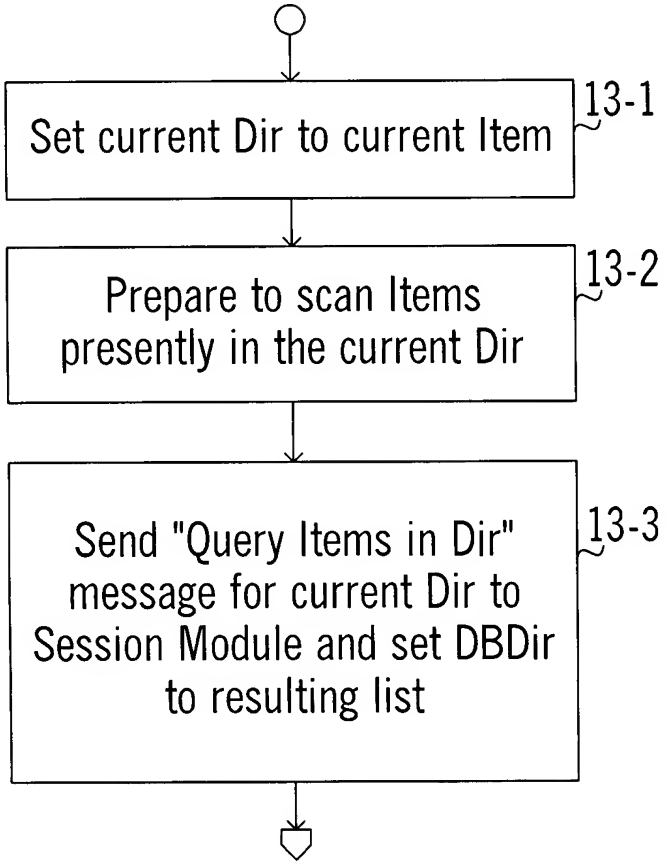

Set current Dir to current Item
13-1
Prepare to scan Items presently in the current Dir
13-2
Send "Query Items in Dir" message for current Dir to Session Module and set DBDir to resulting list
13-3

FIG. 13

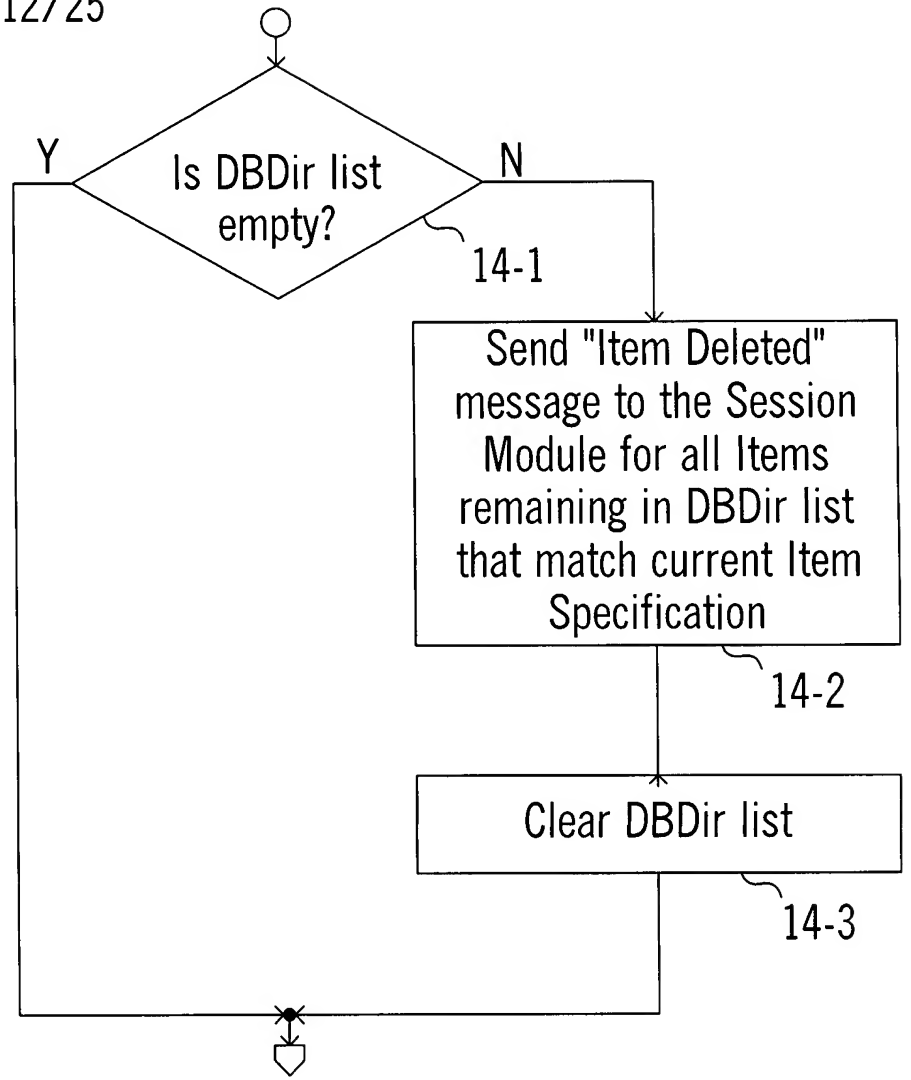

Y
Is DBDir list empty?
N
14-1
Send "Item Deleted" message to the Session Module for all Items remaining in DBDir list that match current Item Specification
14-2
Clear DBDir list
14-3

FIG. 14

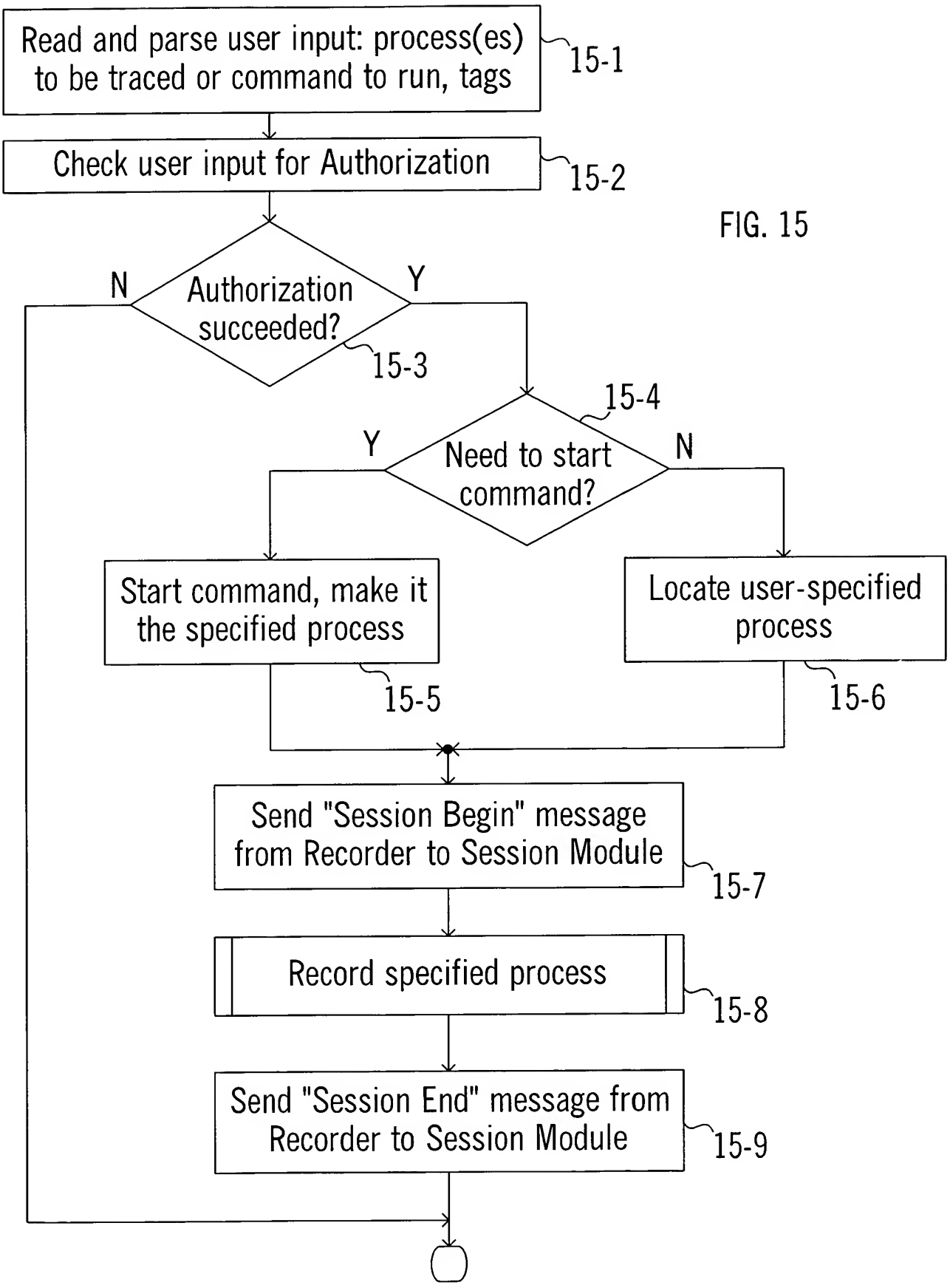

Read and parse user input: process(es) to be traced or command to run, tags
15-1
Check user input for Authorization
15-2
Authorization succeeded?
N
Y
15-3
15-4
Need to start command?
Y
N
Start command, make it the specified process
15-5
Locate user-specified process
15-6
Send "Session Begin" message from Recorder to Session Module
15-7
Record specified process
15-8
Send "Session End" message from Recorder to Session Module
15-9

FIG. 15

FIG. 16

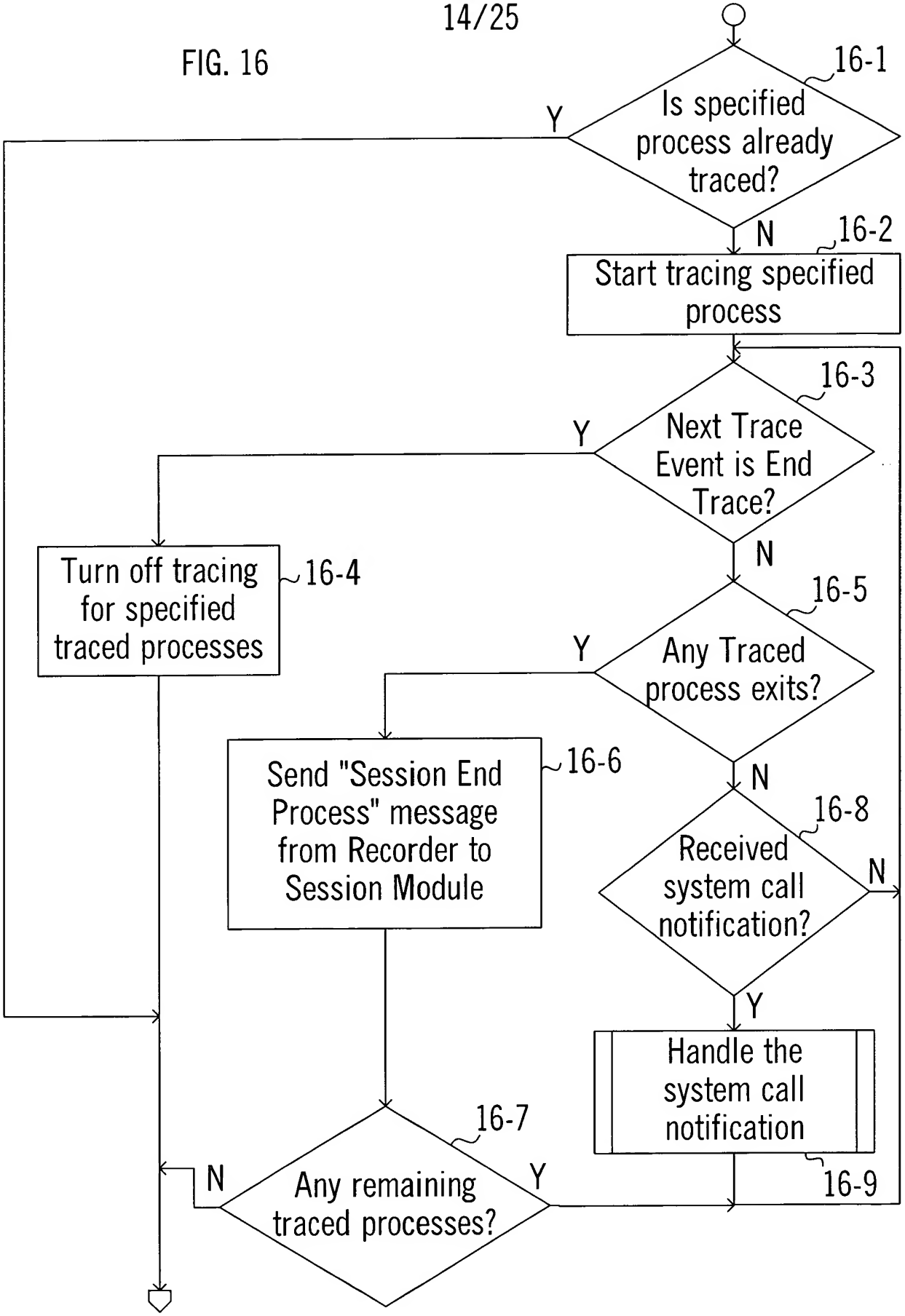
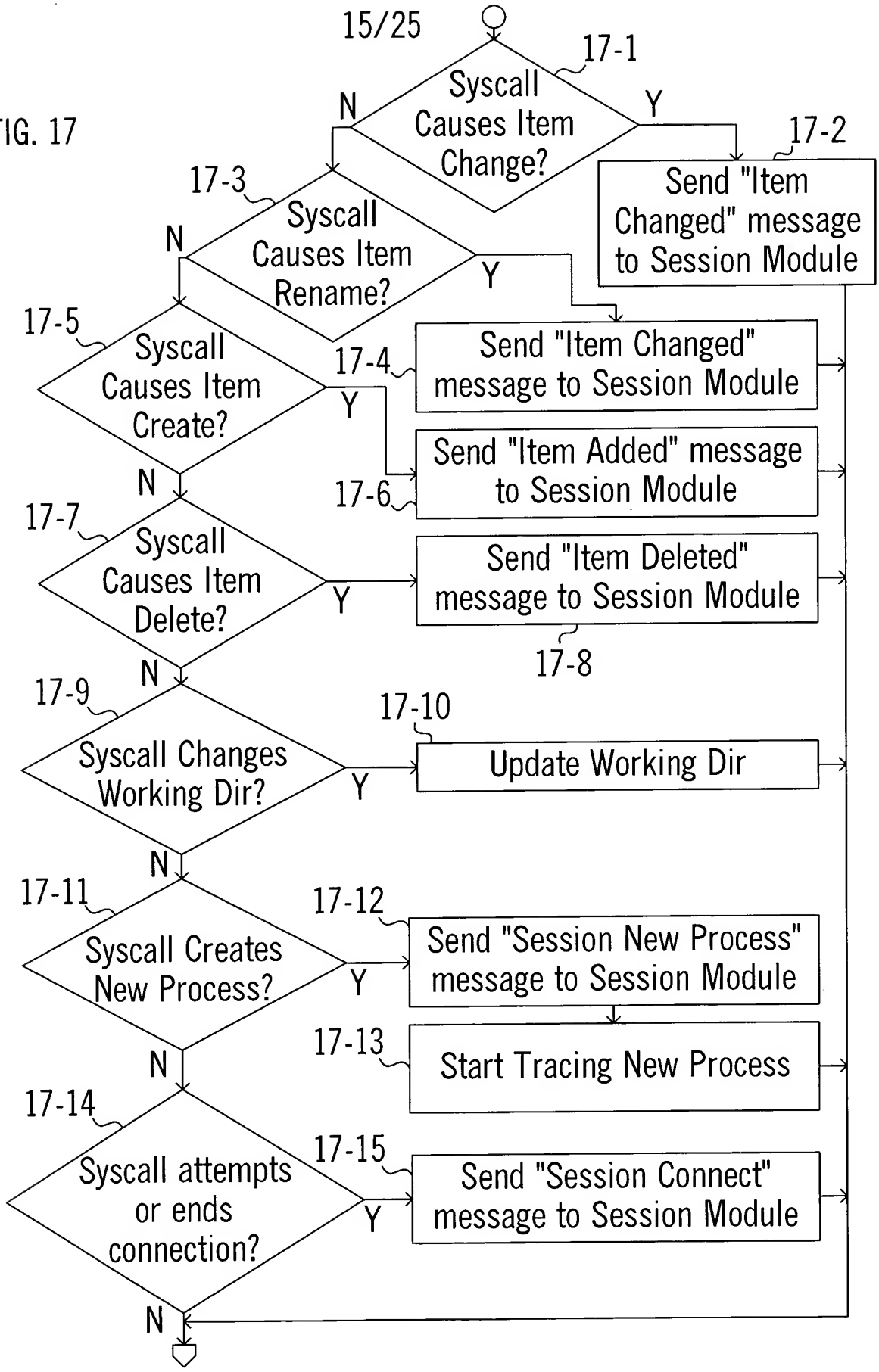

16-1
Is specified process already traced?
Y
N
16-2
Start tracing specified process
16-3
Next Trace Event is End Trace?
Y
N
Turn off tracing for specified traced processes
16-4
16-5
Any Traced process exits?
Y
N
Send "Session End Process" message from Recorder to Session Module
16-6
16-8
Received system call notification?
N
Y
Handle the system call notification
16-9
16-7
Any remaining traced processes?
N
Y

FIG. 17


17-1
Syscall Causes Item Change?
N
Y
17-2
Send "Item Changed" message to Session Module
17-3
Syscall Causes Item Rename?
N
Y
17-4
Send "Item Changed" message to Session Module
17-5
Syscall Causes Item Create?
Y
17-6
Send "Item Added" message to Session Module
N
17-7
Syscall Causes Item Delete?
Y
Send "Item Deleted" message to Session Module
17-8
N
17-9
Syscall Changes Working Dir?
17-10
Y
Update Working Dir
N
17-11
Syscall Creates New Process?
17-12
Y
Send "Session New Process" message to Session Module
17-13
Start Tracing New Process
N
17-14
Syscall attempts or ends connection?
17-15
Y
Send "Session Connect" message to Session Module
N

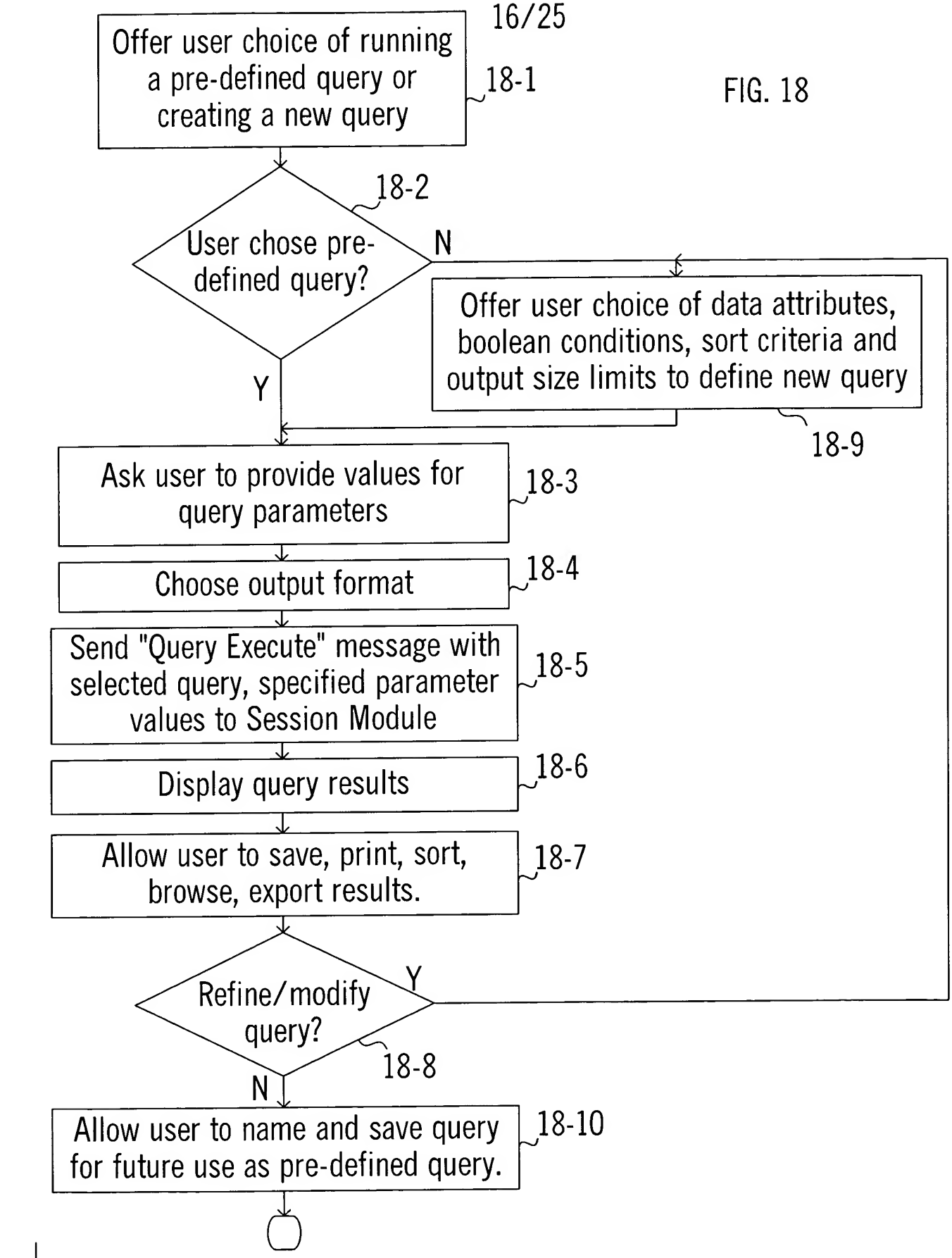
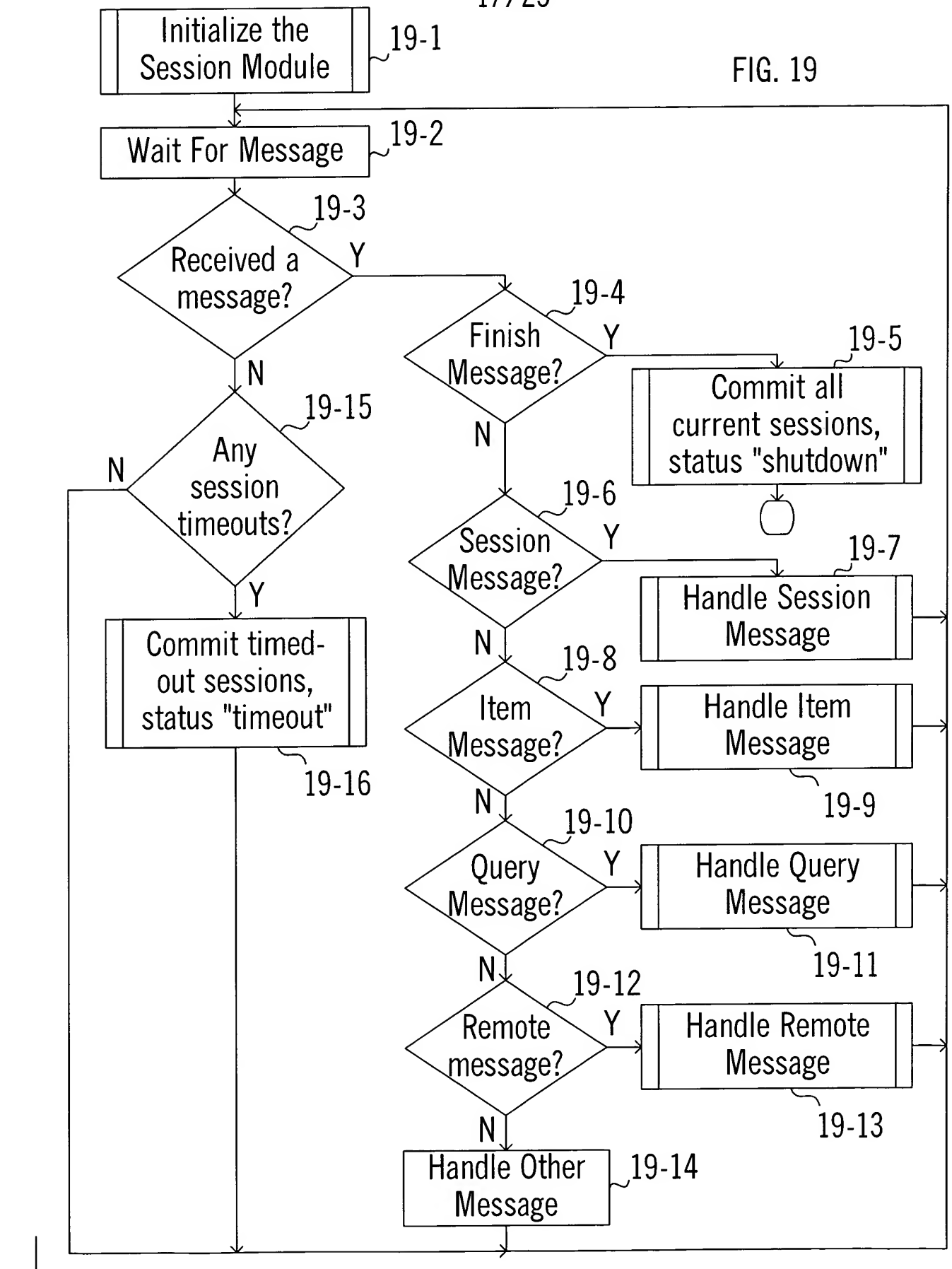

Offer user choice of running a pre-defined query or creating a new query
18-1
User chose pre-defined query?
18-2
N
Y
Offer user choice of data attributes, boolean conditions, sort criteria and output size limits to define new query
18-9
Ask user to provide values for query parameters
18-3
Choose output format
18-4
Send "Query Execute" message with selected query, specified parameter values to Session Module
18-5
Display query results
18-6
Allow user to save, print, sort, browse, export results.
18-7
Refine/modify query?
18-8
Y
N
Allow user to name and save query for future use as pre-defined query.
18-10

FIG. 18

FIG. 19


Initialize the Session Module
19-1
Wait For Message
19-2
Received a message?
19-3
Y
N
Finish Message?
19-4
Y
N
Commit all current sessions, status "shutdown"
19-5
Any session timeouts?
19-15
N
Y
Session Message?
19-6
Y
N
Handle Session Message
19-7
Commit timed-out sessions, status "timeout"
19-16
Item Message?
19-8
Y
N
Handle Item Message
19-9
Query Message?
19-10
Y
N
Handle Query Message
19-11
Remote message?
19-12
Y
N
Handle Remote Message
19-13
Handle Other Message
19-14

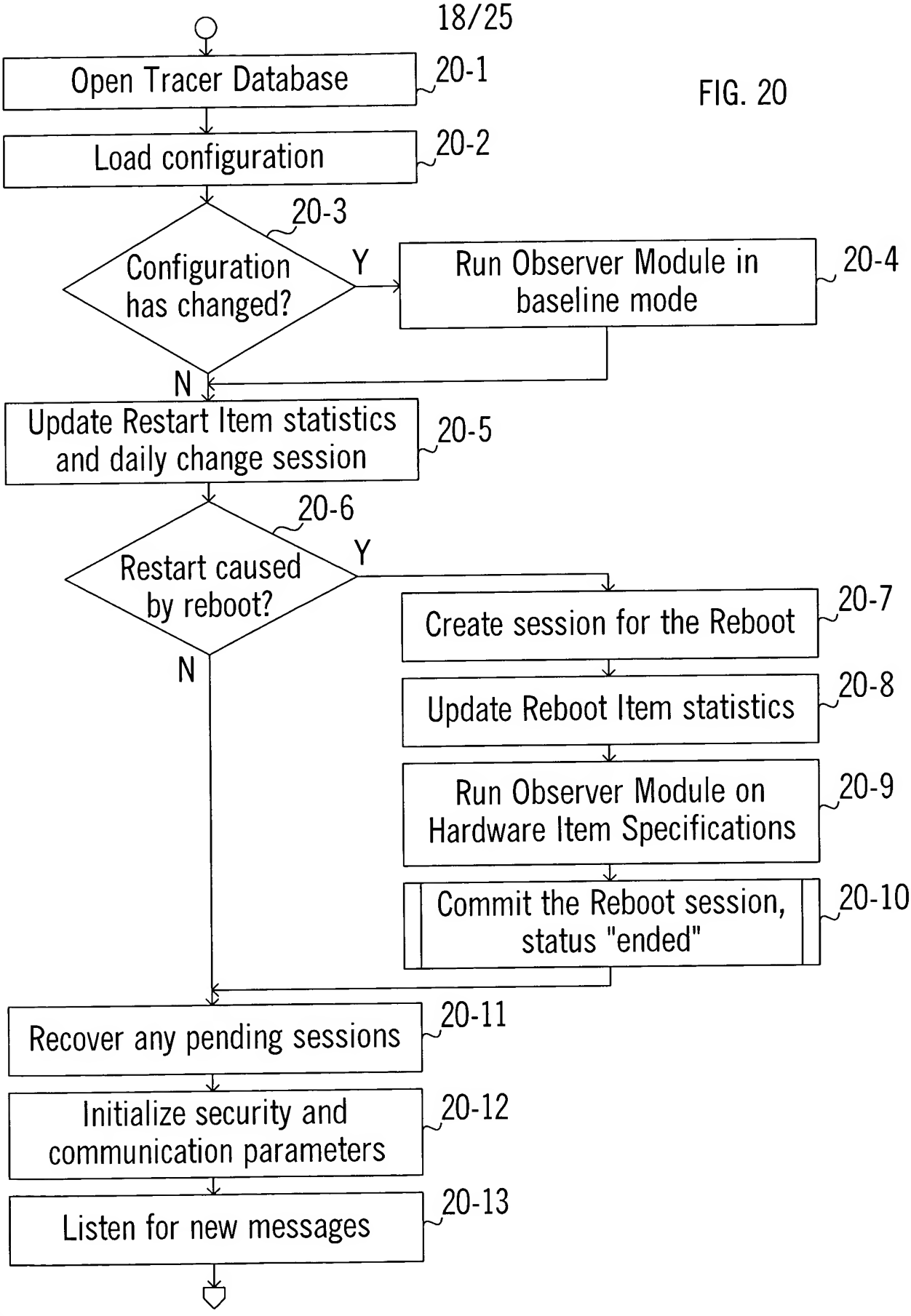

Open Tracer Database
20-1
Load configuration
20-2
20-3
Configuration has changed?
Y
Run Observer Module in baseline mode
20-4
N
Update Restart Item statistics and daily change session
20-5
20-6
Restart caused by reboot?
Y
Create session for the Reboot
20-7
N
Update Reboot Item statistics
20-8
Run Observer Module on Hardware Item Specifications
20-9
Commit the Reboot session, status "ended"
20-10
Recover any pending sessions
20-11
Initialize security and communication parameters
20-12
Listen for new messages
20-13

FIG. 20

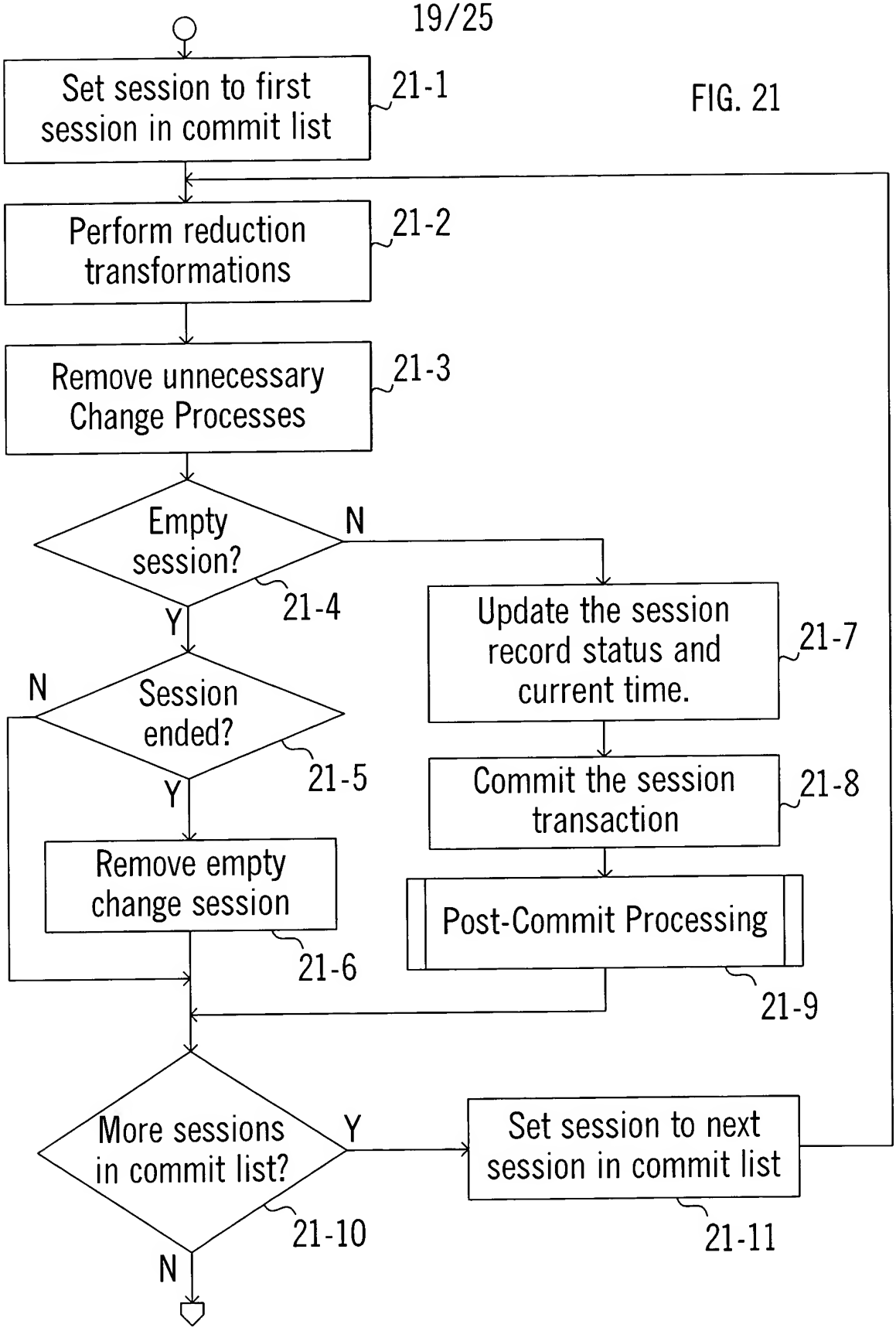

Set session to first session in commit list
21-1
Perform reduction transformations
21-2
Remove unnecessary Change Processes
21-3
Empty session?
21-4
N
Y
Session ended?
21-5
N
Y
Remove empty change session
21-6
Update the session record status and current time.
21-7
Commit the session transaction
21-8
Post-Commit Processing
21-9
More sessions in commit list?
21-10
Y
N
Set session to next session in commit list
21-11

FIG. 21

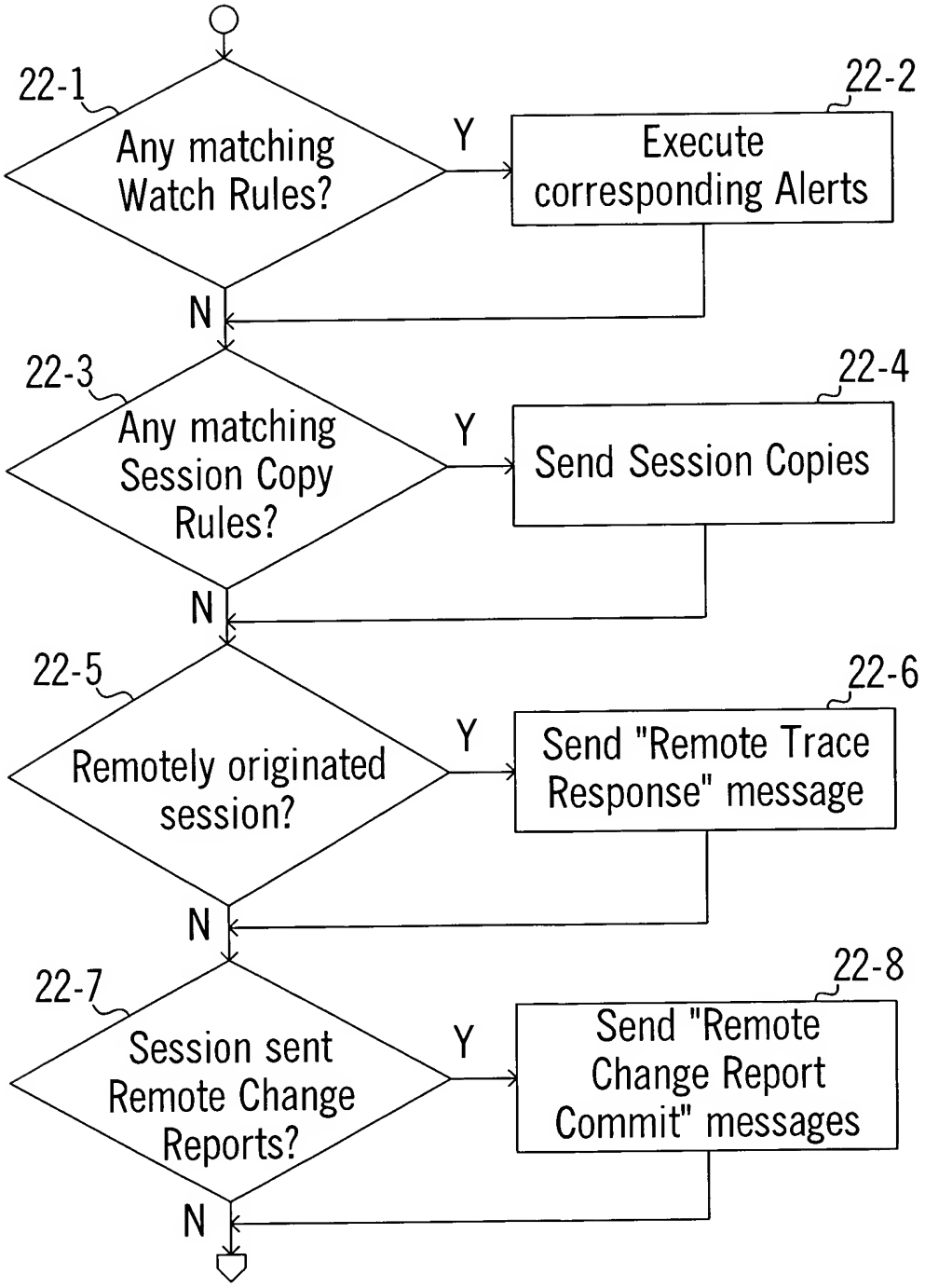
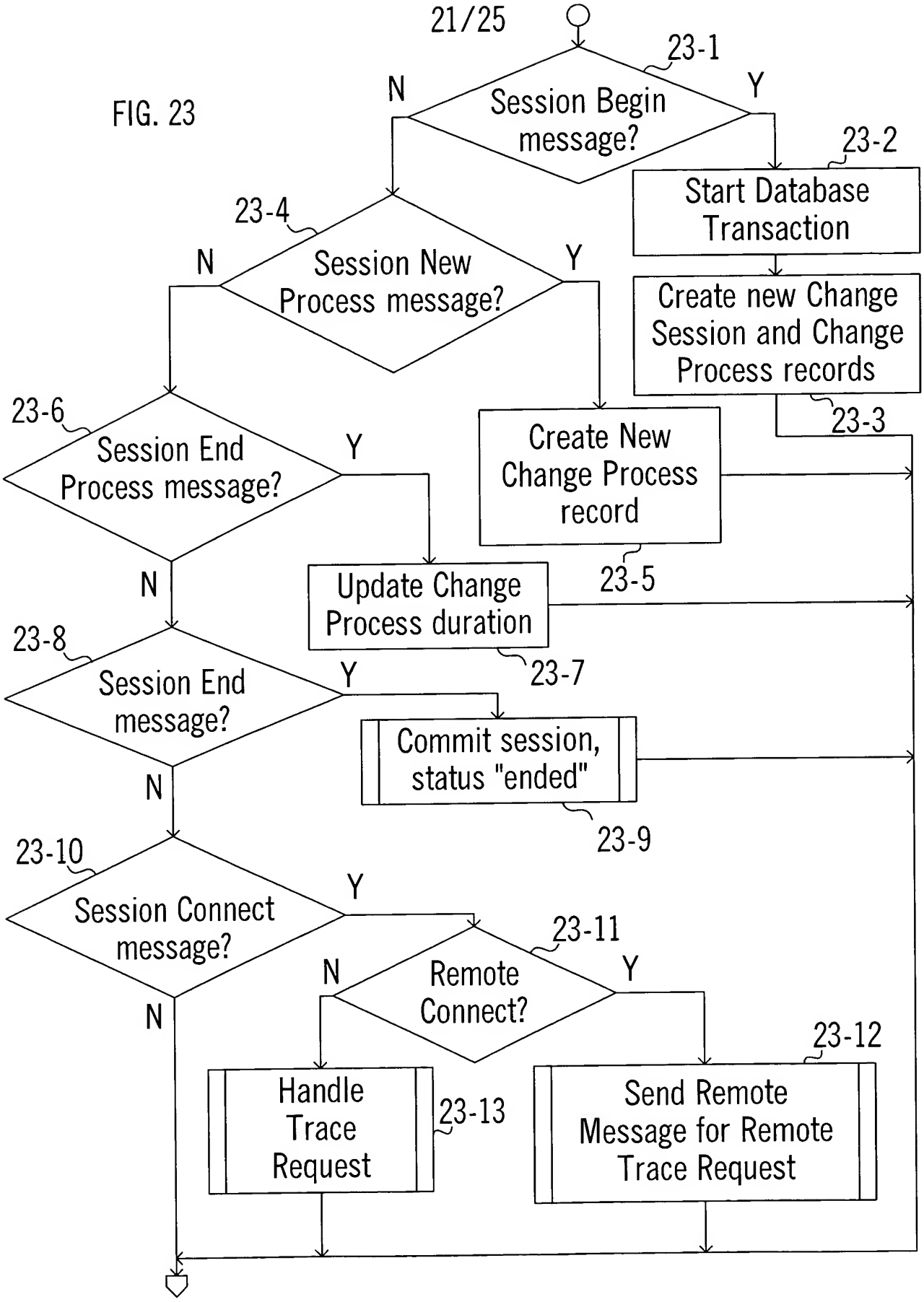

22-1
Any matching Watch Rules?
Y
22-2
Execute corresponding Alerts
N
22-3
Any matching Session Copy Rules?
Y
22-4
Send Session Copies
N
22-5
Remotely originated session?
Y
22-6
Send "Remote Trace Response" message
N
22-7
Session sent Remote Change Reports?
Y
22-8
Send "Remote Change Report Commit" messages
N

FIG. 22

FIG. 23


23-1
Session Begin message?
N
Y
23-2
Start Database Transaction
23-4
Session New Process message?
N
Y
Create new Change Session and Change Process records
23-3
23-6
Session End Process message?
Y
Create New Change Process record
N
Update Change Process duration
23-5
23-7
23-8
Session End message?
Y
Commit session, status "ended"
23-9
N
23-10
Session Connect message?
Y
23-11
Remote Connect?
N
Y
N
23-12
Handle Trace Request
23-13
Send Remote Message for Remote Trace Request

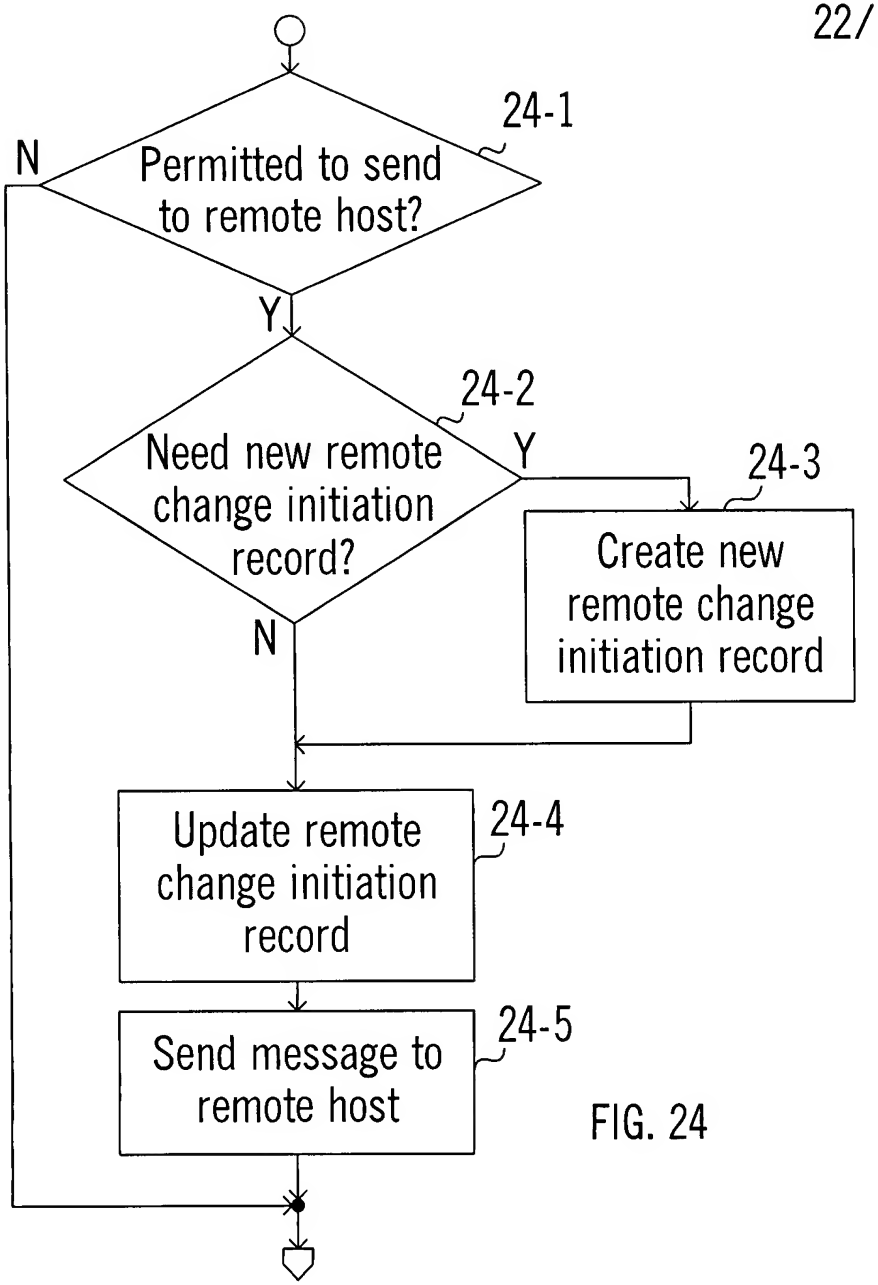

Permitted to send to remote host?
24-1
N
Y
Need new remote change initiation record?
24-2
Y
N
Create new remote change initiation record
24-3
Update remote change initiation record
24-4
Send message to remote host
24-5

FIG. 24

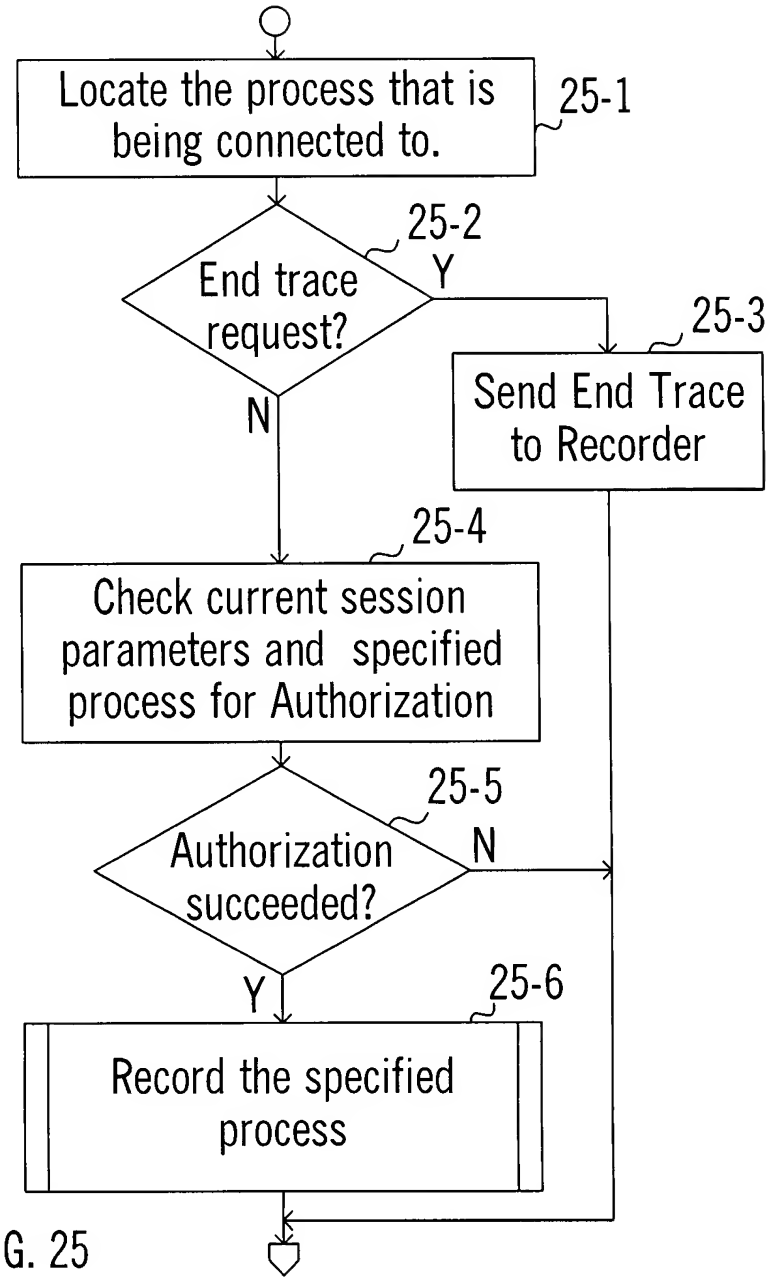
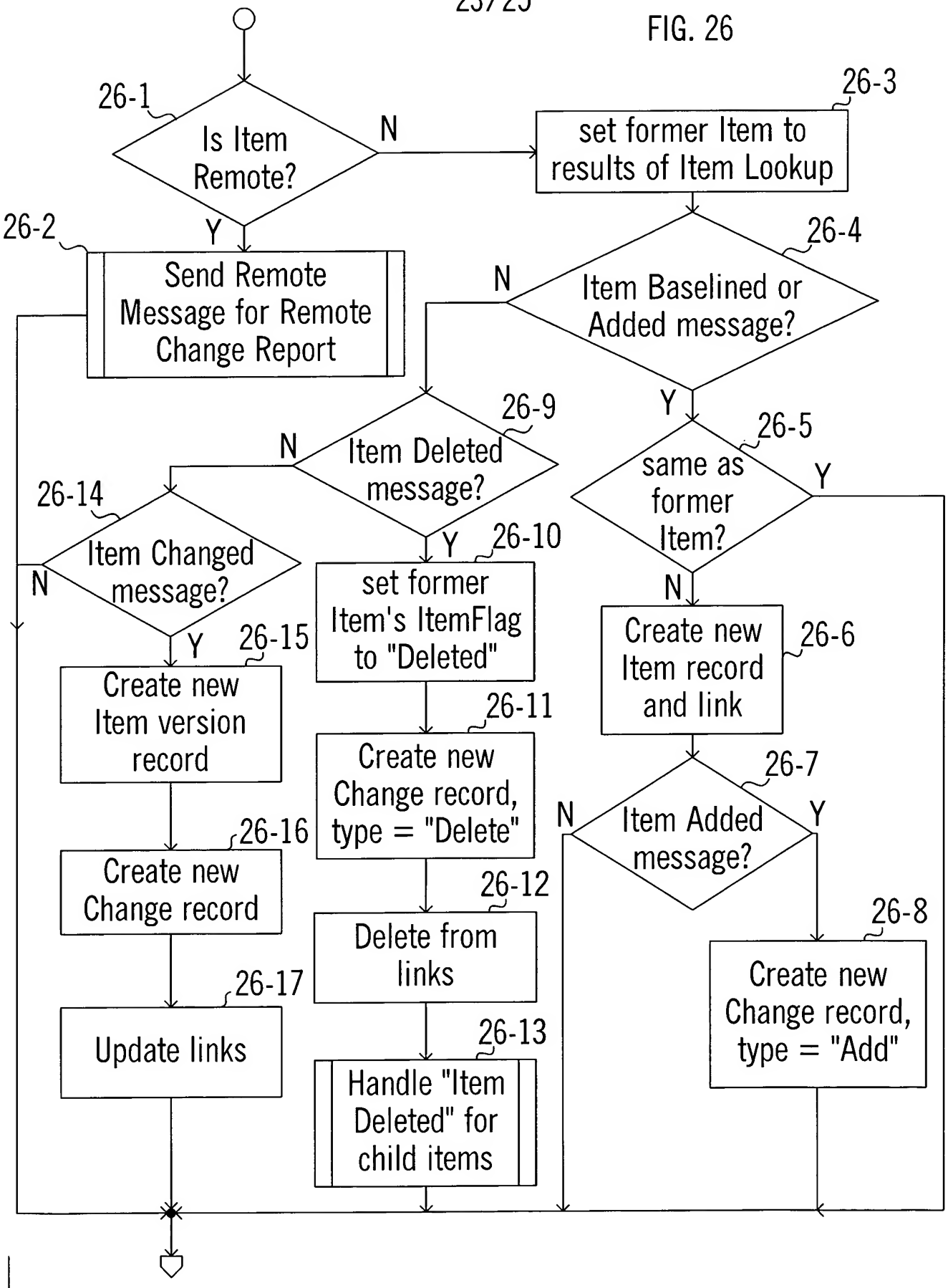

Locate the process that is being connected to.
25-1
End trace request?
25-2
Y
N
Send End Trace to Recorder
25-3
Check current session parameters and specified process for Authorization
25-4
Authorization succeeded?
25-5
N
Y
Record the specified process
25-6

FIG. 25

FIG. 26


26-1
Is Item Remote?
N
26-3
set former Item to results of Item Lookup
Y
26-2
Send Remote Message for Remote Change Report
26-4
Item Baselined or Added message?
N
Y
26-9
Item Deleted message?
N
26-5
same as former Item?
Y
26-14
Item Changed message?
N
Y
26-10
set former Item's ItemFlag to "Deleted"
N
Create new Item record and link
26-6
Y
26-15
Create new Item version record
26-11
Create new Change record, type = "Delete"
26-7
Item Added message?
N
Y
26-16
Create new Change record
26-12
Delete from links
26-8
Create new Change record, type = "Add"
26-17
Update links
26-13
Handle "Item Deleted" for child items

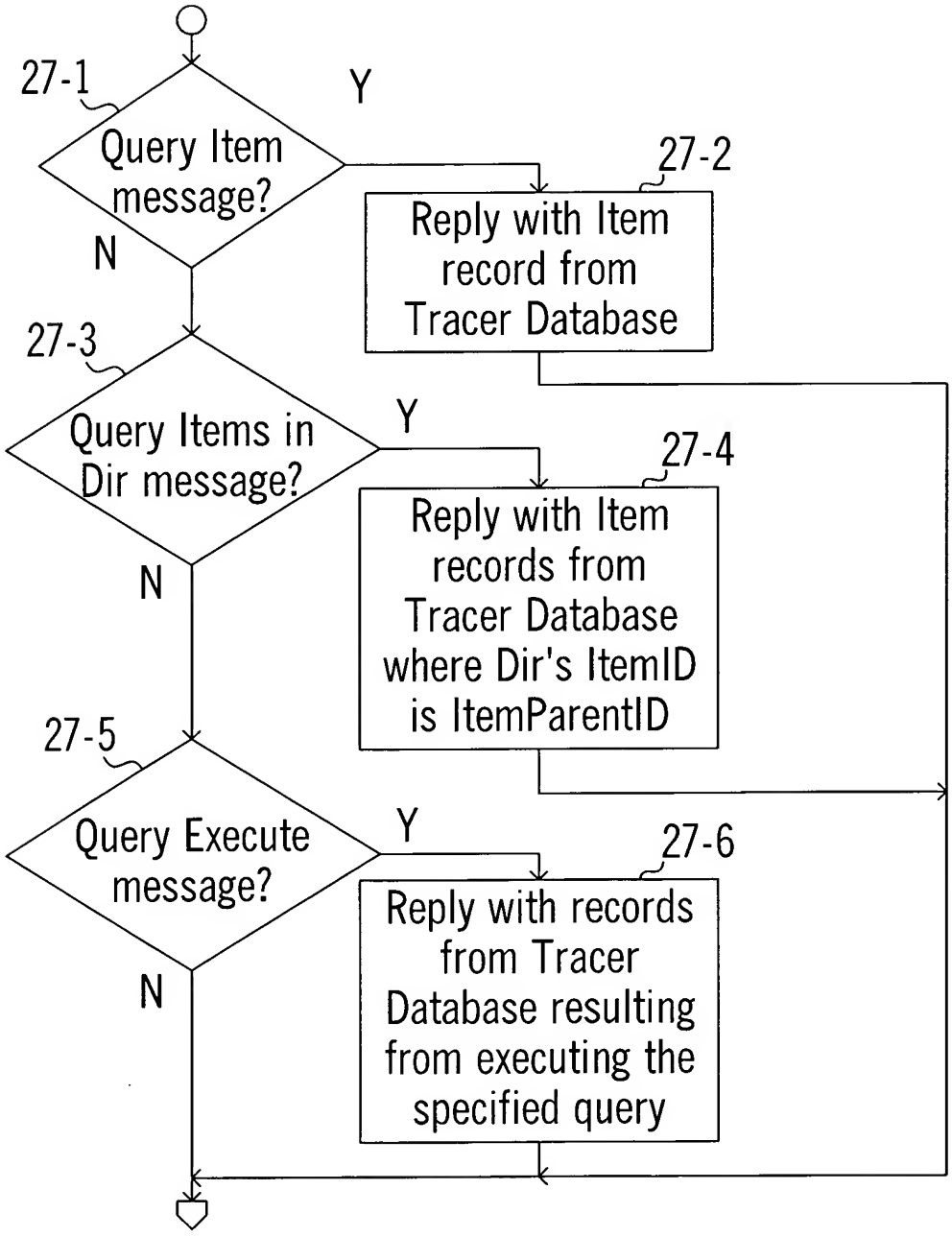
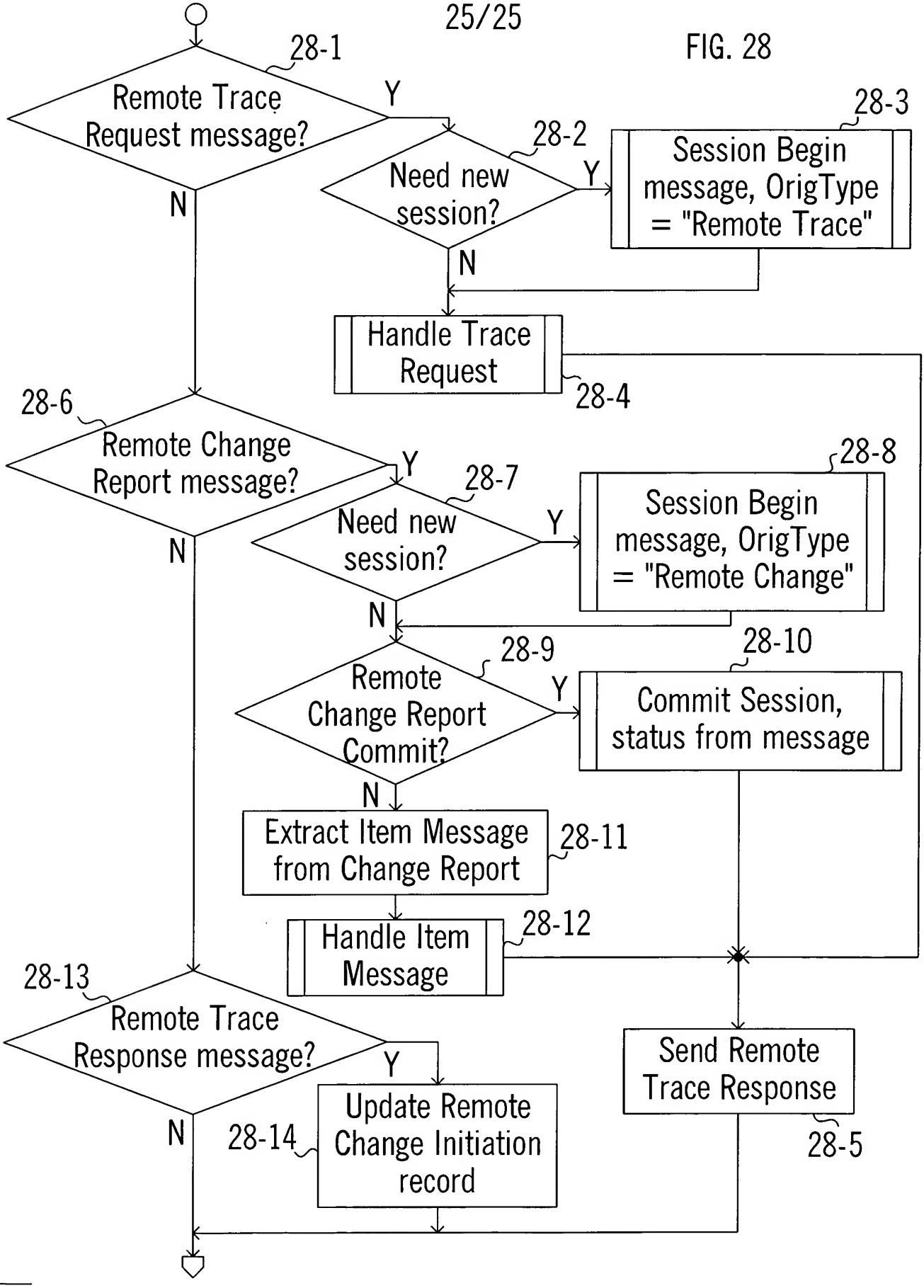

27-1
Query Item message?
Y
N
27-2
Reply with Item record from Tracer Database
27-3
Query Items in Dir message?
Y
N
27-4
Reply with Item records from Tracer Database where Dir's ItemID is ItemParentID
27-5
Query Execute message?
Y
N
27-6
Reply with records from Tracer Database resulting from executing the specified query

FIG. 27

FIG. 28


28-1
Remote Trace Request message?
Y
N
28-2
Need new session?
Y
N
28-3
Session Begin message, OrigType = "Remote Trace"
Handle Trace Request
28-4
28-6
Remote Change Report message?
Y
N
28-7
Need new session?
Y
N
28-8
Session Begin message, OrigType = "Remote Change"
28-9
Remote Change Report Commit?
Y
N
28-10
Commit Session, status from message
Extract Item Message from Change Report
28-11
Handle Item Message
28-12
28-13
Remote Trace Response message?
Y
N
28-14
Update Remote Change Initiation record
Send Remote Trace Response
28-5